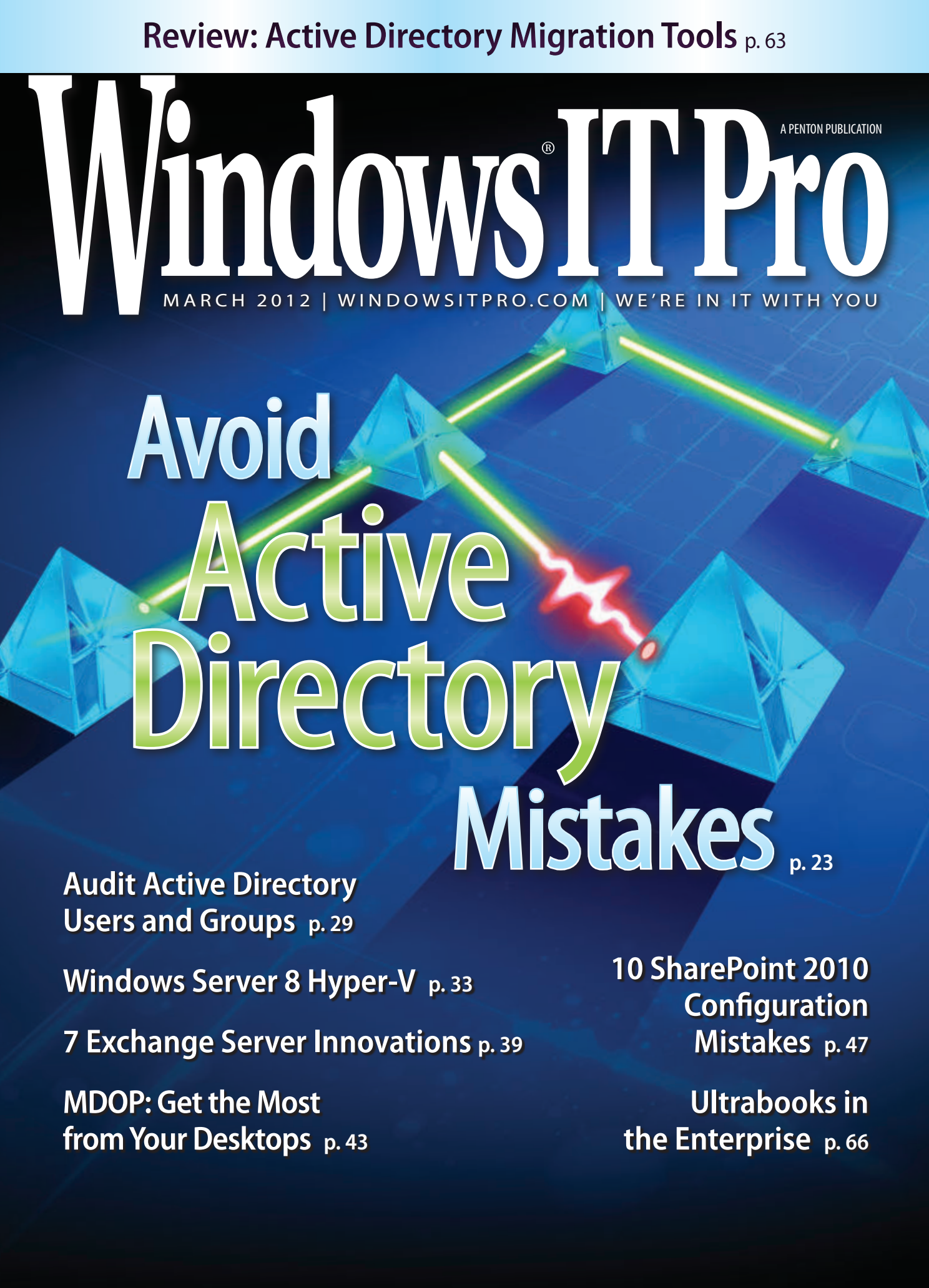
Review: Active Directory Migration Tools p. 63

Windows IT Pro

A PENTON PUBLICATION

MARCH 2012 | WINDOWSITPRO.COM | WE'RE IN IT WITH YOU



Avoid Active Directory Mistakes p. 23

Audit Active Directory Users and Groups p. 29

Windows Server 8 Hyper-V p. 33

7 Exchange Server Innovations p. 39

MDOP: Get the Most from Your Desktops p. 43

10 SharePoint 2010 Configuration Mistakes p. 47

Ultrabooks in the Enterprise p. 66

C O N T E N T S

COVER STORY

23 Avoid Active Directory Mistakes in Windows Server 2008
If you're planning to upgrade your Windows Server 2003 domain controllers, follow these tips to avoid potential problems with installation and virtual machines.
BY JUSTIN HALL

FEATURES

29 4 Challenges of Auditing Active Directory Users and Groups
Use this PowerShell script to create a list of users and their group memberships, in record time.
BY BILL STEWART

33 Windows Server 8 Hyper-V
New high-availability and migration features put Hyper-V ahead of the pack when it comes to machine virtualization.
BY JOHN SAVILL

39 7 Important Exchange Server Innovations
Microsoft Exchange Server has evolved from its humble origins as a LAN-based email server into a messaging giant that spans on-premises servers as well as the cloud. Several technical advances made this growth possible and matter most to today's Exchange admins and users.
BY TONY REDMOND

43 Get the Most from Your Desktops with MDOP
Windows 7 Enterprise offers plenty of enhanced features for desktop users. The OS also offers an improved management experience, through the most recent version of the Microsoft Desktop Optimization Pack.
BY JOHN SAVILL

47 Top 10 SharePoint 2010 Configuration Mistakes
If SharePoint 2010 is giving you trouble, the culprit might be one of several common configuration errors. Fortunately, fixing these issues can be quick and painless.
BY TODD O. KLINDT

INTERACT

15 Reader to Reader
Remove orphaned icons in disk utilities, and boot Windows 8 from a Virtual Hard Disk (VHD) in Windows 7.

17 Ask the Experts
Get expert help with Microsoft Outlook rules creation, SQL Server database shrinking, virtualization, and more.

IN EVERY ISSUE

Access articles online at www.windowsitpro.com. Enter the article ID (located at the end of each article) in the Search box on the home page.

Windows IT Pro
A PENTON PUBLICATION
MARCH 2012
VOLUME_18 NO_3

COLUMNS

OTEY | IT PRO PERSPECTIVES

3 Virtualization Trends in 2012
Expect continued server consolidation, more VDI and application virtualization, and support for the dynamic data center and private cloud.

THURROTT | NEED TO KNOW

7 Windows 8 Hardware Certification Requirements, and What Happened to Drive Extender in Windows 8
Learn more about Windows 8 storage-related features; plus, see what Microsoft is requiring for Windows 8 hardware certification—you might be surprised.

MINASI | WINDOWS POWER TOOLS

10 Search-ADAccount and the Missing 15 Days
Search-adaccount can tell you which users' accounts are inactive. Get to know its syntax, as well as an interesting idiosyncrasy Mark calls "the missing 15 days of *search-adaccount*."

OTEY | TOP 10

11 New Features in SQL Server 2012
Enhanced high availability heads the list of SQL Server 2012 improvements, but you'll also find features for better performance, easier business intelligence (BI), simplified licensing, and a streamlined number of editions.

DEUBY | ENTERPRISE IDENTITY

12 Identity Predictions
Two sessions related to Active Directory at the Gartner Identity and Access Management Summit provide rich food for thought in the identity realm.

C O N T E N T S

PRODUCTS

Windows IT Pro

EDITORIAL

Editor in Chief
Amy Eisenberg amy@windowsitpro.com

Senior Technical Director
Michael Otey motey@windowsitpro.com

Technical Director
Sean Deuby sean@windowsitpro.com

Senior Technical Analyst
Paul Thurrott paul@windowsitpro.com

Industry News Analyst
Jeff James jjames@windowsitpro.com

Custom Group Editorial Director
Dave Bernard dbernard@windowsitpro.com

Exchange & Outlook
Brian Winstead bwinstead@windowsitpro.com

Systems Management, Networking, Hardware
Jason Bovberg jbovberg@windowsitpro.com

Security, Virtualization
Jeff James jjames@windowsitpro.com

SharePoint
Caroline Marwitz cmarwitz@windowsitpro.com

SQL Server, Developer Content
Megan Keller mkeller@windowsitpro.com

Managing Editor
Lavon Peters lavon.peters@penton.com

Editorial SEO Specialist
Jayleen Heft jayleen.heft@penton.com

Editorial Assistant
Blair Greenwood blair.greenwood@penton.com

CONTRIBUTORS

SharePoint and Office Community Editor
Dan Holme danh@intelliem.com

Senior Contributing Editors
David Chernicoff david@windowsitpro.com
Mark Minasi mark@minasi.com
Paul Robichaux paul@robichaux.net
Mark Russinovich mark@sysinternals.com
John Savill john@savilltech.com

Contributing Editors
Alex K. Angelopoulos aka@mvps.org
Michael Dragone mike@mikerochip.com
Jeff Fellinge jeff@blackstatic.com
Brett Hill brett@iisanswers.com
Darren Mar-Elia dmarelia@windowsitpro.com
Tony Redmond 12knocksinna@gmail.com
Eric B. Rux ericbrux@whshelp.com
William Sheldon bsheldon@interknowlogy.com
Curt Spanburgh cspanburgh@scg.net
Orin Thomas orin@windowsitpro.com
Douglas Toombs help@toombs.us
Ethan Wilansky ewilansky@windowsitpro.com

ART & PRODUCTION

Production Director
Linda Kirchgesler linda@windowsitpro.com

Senior Graphic Designer
Matt Wiebe matt.wiebe@penton.com

ADVERTISING SALES

Publisher
Peg Miller pmiller@windowsitpro.com

Director of IT Strategy and Partner Alliances
Birdie J. Ghiglione birdie.ghiglione@penton.com
619-442-4064

Manager of IT and Dev Strategy and Partner Alliance
Marie Evans marie.evans@penton.com
970-203-2761

Online Sales Development Director
Amanda Phillips amanda.phillips@penton.com
970-203-2761

Key Account Director
Chrissy Ferraro christina.ferraro@penton.com
970-203-2883

Account Executives
Barbara Ritter barbara.ritter@penton.com
858-367-8058
Cass Schulz cassandra.schulz@penton.com
858-357-7649

Client Project Managers
Michelle Andrews 970-613-4964
Kim Eck 970-203-2953

Ad Production Supervisor
Glenda Vaught glenda.vaught@penton.com

MARKETING & CIRCULATION

Customer Service service@windowsitpro.com

Marketing Director
Sandy Lang sandy.lang@penton.com

CORPORATE

PENTON

Chief Executive Officer
David Kieselstein david.kieselstein@penton.com

Chief Financial Officer/Executive Vice President
Nicola Allais nicola.allais@penton.com

TECHNOLOGY GROUP

Senior Vice President, Technology Media Group
Kim Paulsen kpaulsen@windowsitpro.com

WRITING FOR *WINDOWS IT PRO*
Submit queries about topics of importance to Windows managers and systems administrators to articles@windowsitpro.com.

LIST RENTALS
Contact MeritDirect, 333 Westchester Avenue, White Plains, NY or www.meritdirect.com/penton.

REPRINTS
Wright's Media
penton@wrightsmedia.com 877-652-5295

Otey

"Expect to see the continued virtualization of larger and larger workloads."

Virtualization Trends in 2012

It wasn't all that long ago that virtualization was viewed as cutting edge technology that was useful for development and testing but not for real production implementations. But the advent of hypervisor-based virtualization technologies like VMware's ESX Server and Microsoft's Hyper-V Server radically changed that perception.

These technologies moved the support of the virtualization layer out of the OS and put it directly on the system hardware, vastly improving the performance and stability of virtual machines (VMs). In addition, hardware improvements like 64-bit processors and, more recently, support for Second Level Address Translation (SLAT) have significantly boosted the scalability and performance that are available for VMs. Virtualization is now a core IT infrastructure technology. In 2012, expect to see the continued virtualization of larger and larger workloads.

One of the important virtualization trends that larger companies are pursuing is Virtual Desktop Infrastructure (VDI), also called Hosted Desktop Virtualization. VDI should not be confused with desktop virtualization products like VMware Workstation or Microsoft's Virtual PC, where the virtualization software runs on the desktop itself. With VDI, the virtualization support is provided by a back-end virtual server product such as VMware's ESX Server or Microsoft's Hyper-V. The physical client machine in a VDI implementation requires very little processing power and can be a legacy PC or even a thin client. The client needs only enough power to run a remote connection protocol like RDP or ICA, which is routed to a target VM image running off the back-end virtualization server. VDI provides greatly improved central management of clients as well as easy migration to new client OSs because VDI eliminates the need to physically upgrade the client machines. Popular VDI products include VMware's View and Citrix's XenDesktop.

A trend that's popular in larger companies is application virtualization. Because virtualized applications must be preprocessed before they can be deployed, application virtualization isn't used as much by smaller organizations that don't want to deal with the complexity. The two main application virtualization products are VMware's ThinApp and Microsoft's App-V. Application virtualization makes it easy to deploy new applications, and because the applications are essentially sandboxed, they don't need to be installed on the client to run nor will they interfere with other applications that might be on the client desktop. IT assigns virtualized applications to users in Active Directory (AD). Then, when the user logs on, the virtualized application is streamed to the user.

Probably the most important virtualization trend that lays the groundwork for the future is support for the dynamic datacenter. Most organizations are already taking advantage of virtualization for server consolidation. The next step is the ability to move virtualized resources between different hosts with no downtime. Many organizations are using technologies like VMotion and Live Migration to accomplish this task. The dynamic datacenter builds on this foundation by automatically moving workloads between virtualization hosts based on demand or resource utilization. Products like VMware's Distributed Resource Scheduler (DRS), Microsoft System Center Virtual Machine Manager (SCVMM) 2008's Performance Resource Optimization (PRO) feature, or VMM 2012's Dynamic Optimization let an organization add dynamic workload optimization onto its existing virtual infrastructure.

You can't write about virtualization today and not cover the cloud somewhere. The institution of the dynamic datacenter paves the way to the private cloud. Using virtualization to create the private cloud is the most recent and perhaps most important virtualization trend in 2012. The private cloud is more than just virtualization. Virtualization and the ability to dynamically move VMs and resources between hosts provide the foundation for the private cloud. However, the private cloud adds the ability to create resource pools from virtualized assets, manage multiple VMs as a single unit or service, and provide self-service capabilities and usage-based resource metering. The private cloud increases IT's flexibility and enables it to respond to user requests more rapidly. Microsoft's VMM 2012 and VMware's vCloud Director allow you to build private cloud infrastructures. Today, implementing the private cloud is a small but growing trend that may well be the next standard for building IT infrastructure.

InstantDoc ID 142011

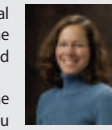
MICHAEL OTEY (motey@windowsitpro.com) is senior technical director for *Windows IT Pro* and *SQL Server Pro* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Windows IT Pro is going digital!

We're excited to announce that, starting in May, we'll be offering an upgraded digital edition with enhanced multimedia and social media content. The new digital editions will replace the print magazine, providing the same great content now enhanced with audio and video, social media feeds, and other interactive features.

We look forward to continuing to provide in-depth technical content that you can now view on your PC, tablet, or smartphone device. You'll be able to read the digital edition online or offline, and you'll have the ability to print articles on demand.

In the coming months we'll be rolling out tablet and smartphone apps, so let us know what features we can provide that will help you do your job more effectively. Thanks for reading and being part of the *Windows IT Pro* community!



—Amy Eisenberg, Editor in Chief

MARCH 26-29, 2012 • MGM GRAND • LAS VEGAS, NEVADA

CLOUD CONNECTIONS
WINDOWS CONNECTIONS
UNIFIED COMMUNICATIONS CONNECTIONS
Microsoft® Exchange CONNECTIONS
SharePoint CONNECTIONS
SQL Server CONNECTIONS

TAKE THE JOURNEY INTO 2012

WITH MICROSOFT & INDUSTRY EXPERTS AS NEW TECHNOLOGIES & PRODUCTS RELEASE

Take a deep dive with Microsoft and industry experts into Windows 8, Cloud, SharePoint and Exchange

BONUS:
Connections is excited to be hosting one of the SQL SERVER 2012 LAUNCH EVENTS

SOLUTION ARCHITECTS, SYSTEM AND MESSAGING ADMIN, INFRASTRUCTURE ARCHITECTS, NETWORK ADMIN, CTOS, IT MANAGERS AND DIRECTORS

KEEP YOUR COMPETITIVE EDGE!

KEYNOTES

MARK MINASI
MINASI RESEARCH AND DEVELOPMENT

SCOTT GUTHRIE
MICROSOFT CORPORATE VICE PRESIDENT

SHAWN BICE
MICROSOFT DIRECTOR OF PROGRAM MANAGEMENT

STEVE FOX
MICROSOFT DIRECTOR

PAUL THURROTT
WINDOWS IT PRO MAGAZINE

A sampling of speakers CONFERENCE ADVISORY BOARD

KIMBERLY L. TRIPP
SQLSKILLS.COM

PAUL S. RANDAL
SQLSKILLS.COM

MICHAEL OTEY
WINDOWS IT PRO & SQL SERVER MAGAZINE

CHRIS AVIS
MICROSOFT

SCOT HILLIER
SCOT HILLIER TECHNICAL SOLUTIONS, LLC

SEAN DEUBY
PENTON MEDIA

DON JONES
CONCENTRATED TECHNOLOGY, LLC

JIM MCBEE
ITHICOS SOLUTIONS

ALAN SUGANO
ADS CONSULTING GROUP

...and many more!

FIND US! facebook.com/winconnections

FOLLOW US! twitter.com/winconnect

Register NOW This event will sell out. Space is limited.

REGISTER TODAY! www.WinConnections.com • 800.438.6720 • 203.400.6121

- In Memoriam: Kathy Ivens
- Windows XP
- Windows 8
- Lync Mobile

LETTERS@WINDOWSITPRO.COM

Remembering Kathy Ivens

Kathy Ivens, longtime contributing editor for *Windows IT Pro*, passed away January 16, 2012, at age 70. Readers will likely remember Kathy most for her Reader Challenge column, which she wrote for 13 years. We appreciate Kathy's longstanding dedication to making complex topics accessible and for challenging IT pros to solve common but perplexing problems.

Long Live Windows XP

As a follow-on comment to Jeff James' editorial "Long Live Windows XP" (InstantDoc ID 141341), our reasons for hanging on to XP include all of those that Jeff mentioned in the article and more: It works well and does the job, it isn't bloated, it doesn't force hardware refreshes, we're able to defer relicensing/upgrade fees, the user experience is stable, and there's no need for retraining. All these reasons add up to dollars saved. The only reason we've deployed any Windows 7 platform is that you can't purchase new hardware that will run XP (lack of backward-compatible drivers). Enter terminal services/desktop virtualization—any app, any device.

I work for a heavy manufacturer of durable goods—something that has become more and more difficult to come by for many years—in the northeast United States. We get many visitors to our facility. Often, the first question visitors ask is, "What do you make, exactly?" The glib but most important answer is "Money—continuously for more than 75 years." In my line of business, that's achieved by maintaining continuous process improvements and controlling discretionary expenses. One piece of that is not following the Pied Piper of Redmond in lockstep. Your analysis and future predictions are spot on.

—Dennis Blevins

Windows 8 Top Features

As a computer developer, I think the top 10 features Michael Otey lists in his article "Top 10 New Features in Windows 8" (InstantDoc ID 141257) should be removed. Instead of adding new features, maybe Microsoft should repair the old Windows 7 bugs that Windows 8 will inherit, like waiting (10 to 15 seconds) before the list of network computers appears on the screen. Perhaps the most annoying bug is the displacement of the icons on the desktop almost every time you start the computer.

—Gaetan Lamarre

Lync Mobile Clients

I liked B. K. Winstead's "Lync Mobile Clients from Microsoft Debut" (InstantDoc ID 141642). We've been using Lync 2010 for about a year now and have loved it for our school. We have a remote teacher teaching a math class to our campus. This situation isn't too unusual, except that our students are low-vision and blind. The Lync client was the only product that was accessible for our students.

We also have a group of outreach staff on the road five days a week. They instruct their students in their home school districts across the state of Washington so that students don't need to come to our Vancouver, Washington, campus. Now that the mobile clients are here, we'll be able to communicate with them more easily and will be able to make them feel part of our Vancouver campus.

—Ed Lukowski
InstantDoc ID 142064

Windows IT Pro welcomes feedback about the magazine. Send comments to letters@windowsitpro.com, and include your full name, email address, and daytime phone number. We edit all letters and replies for style, length, and clarity.

Thursday, March 22, 2012

Paul Sheriff

Using WPF for Business Applications eLearning Series from DevProConnections

Creating business applications in Windows Presentation Foundation (WPF) is easy if you know just a few XAML basics. In this seminar we will show you how to make your business applications shine. You will first see lots of different ways that you can use the powerful ListBox. Next you will be shown how to create toolbars, status bars, create add/edit/delete forms and even an application template that you can use as the basis for your WPF applications. Finally you will learn tips and tricks for styling your application using color and styles to make your application really stand out.

http://elearning.left-brain.com/event/using-wpf

Thurrott

"Windows 8 is on a need-to-know basis. And those outside the Windows team simply don't need to know."

Windows 8 Hardware Certification Requirements, and What Happened to Drive Extender in Windows 8

Last month, I discussed some alarming issues concerning Windows 8, Microsoft's curiously still-mysterious coming OS generation (see "Windows 8 Worries," www.windowsitpro.com, InstantDoc ID 141566). Since then, Microsoft has done an admirably lousy job of communicating its plans for Windows 8 to the public and has ignored pleas to reveal its plans. In its final Consumer Electronics Show (CES) keynote address in January, for example, Microsoft didn't discuss any new information about Windows 8 at all, instead reiterating what it had revealed in September 2011, when it delivered the Windows 8 Developer Preview.

The message here, it seems, is that Windows 8 is on a need-to-know basis. And those outside the Windows team simply don't need to know.

I disagree with this pretty strongly, as you might expect, and, in keeping with the name of this column, I intend to keep beating the drum for Windows 8, because, yes, you do need to know. Fortunately, a few nuggets of information have appeared since my last column, and they're quite interesting indeed.

Windows 8 Storage Advances

One of the more exciting areas of improvement in Windows 8—and of course in Windows Server 8 as well—concerns storage. And in the past month, we've learned about some new and interesting storage-related features for these OSs.

You might recall that Microsoft created a technology called Drive Extender, which was designed to somewhat obviate the need for drive letters and to make storage available in flat pools that could be redundant—where crucial data was always copied to two physical disks—and easier to manage. Drive Extender debuted in the original version of Windows Home Server (WHS) but was subsequently removed in WHS 2011, to the dismay of enthusiasts, when Microsoft discovered that it couldn't be fixed to work properly with the server apps that would run on top of WHS-based products such as Windows Small Business Server 2011 Essentials.

This was a problem because the original plan for Drive Extender was to move this technology to the mainstream Windows Server versions, then ultimately to the Windows client, too. Today, Drive Extender lives, sort of, as a new feature of Windows 8 and Windows Server 8, called Storage Spaces. Thematically identical to Drive Extender but architecturally more modern, Storage Spaces lets you organize storage on physical disks in pools. These pools can use storage from any number of different sizes and types of disks, and expanding a storage pool is as simple as adding a new disk. As with Drive Extender, Storage Spaces also provides redundancy, but you can configure that redundancy, through mirroring or parity, to occur across two or more disks (instead of Drive Extender's two).

Storage Spaces can also work with virtualized storage, which is dynamic storage contained in virtual hard disks (VHDs). Virtualized storage provides what Microsoft calls thin provisioning, since it allows an application to grab storage dynamically (i.e., the physical space used by the VHD grows only as it's actually used) rather than take all of the space it might need from the moment it runs. It's unclear how much usage this capability will get, however, given the cheap storage prices we're seeing these days.

But there's more. NTFS is being bolstered with support for very large capacity hard drives, which Microsoft defines as disks larger than 2.2TB, and the ability to use that space more efficiently through larger disk sector sizes. Some of this functionality will require newer PCs with Unified Extensible Firmware Interface (UEFI) firmware instead of now-obsolete BIOS firmware.

And Microsoft's not stopping with NTFS. In Windows Server 8 only, a new file system, called ReFS, for Resilient File System, improves on NTFS in key ways. Most crucially, it includes anti–data-corruption capabilities, is optimized for high-end scaling needs, and, when used in tandem with Storage Spaces, can provide a full end-to-end resiliency architecture.

In keeping with previous file system evolutions, ReFS is aimed only at a single workload—file serving—and will improve over time. As such, it comes with serious limitations in this first version, and it can't be used on a server's boot partition or with removable media of any kind. Microsoft expects to eventually deliver ReFS to the Windows client—though it didn't specify if this would occur in a Windows 8 service pack or other update, or via Windows 9—then allow it to be used as a boot volume.

Windows 8 Logo Certification Requirements

In December 2011, Microsoft quietly published a set of Windows 8 hardware certification requirements aimed at PC makers and, of course, a new generation of ARM-based Windows 8 device makers as well. These documents, which cover devices, filter drivers, and client and server systems, respectively, are a wellspring of

interesting information. But it wasn't until a month after their release that anyone noticed.

Oddly enough, the open-source crowd noticed first. What they found (predictably) but then misrepresented (even more predictably) was a note about a supposed design goal of locking out Linux on ARM-based Windows 8 devices. Let's focus on the real news: some of the more interesting requirements that Microsoft is enforcing for hardware makers who want a certified-for-Windows-8 logo on their devices.

This information was first published by my *Windows 8 Secrets* coauthor Rafael Rivera on his Within Windows blog (within windows.com). Some of the requirements are surprising.

NFC. Windows 8 tablets and other touch-based devices that implement the emerging near field communication (NFC) technology must provide an obvious and visible touch point on the outside of the device. This will make it easier for users to facilitate an NFC-based radio "conversation," if you will, which is a next-generation version of the infrared intra-device communications solutions we futzed with a decade ago. But NFC promises grander possibilities than infrared, including a way for users to make mobile payments at retail stores and other locations.

Digitizers. With touch-based Windows 7, PC makers can implement pretty low-resolution digitizers and only need to support one touch point to get the logo. In Windows 8, they'll be required to support at least five touch points, just the right amount for every finger on a hand. Modern PCs will likely support even more, and Lenovo has already announced a Windows 8–era convertible PC called the IdeaPad YOGA that will support ten touch points.

Hardware buttons. If you're familiar with Windows Phone, you know that handsets based on this mobile OS must include the following hardware buttons: Back, Start, and Search on the front, and Volume, Power, and Camera on the outside edge. Similarly, Windows 8 devices—tablets and convertible PCs—have to implement a stock set of hardware buttons too: Power, Rotation Lock, Windows Key (the WinKey button, not the Windows button or Start button), Volume Up, and Volume Down.

CTRL+ALT+DEL button shortcut. PC enthusiasts know that this keyboard shortcut came to be because Microsoft developers wanted a way of halting application execution and chose a keyboard combination no one would ever hit by mistake. Years later, it's one of the most frequently used keyboard combinations, partly because Microsoft made it a requirement to log on to domain-joined Windows PCs. But what about tablets? In Windows 8, you'll be able to tap Windows Key+Power to emulate CTRL+ATL+DEL, no physical keyboard required.

Tablet and convertible PC minimum requirements. Although today's PCs offer an embarrassment of riches when it comes to computing resources, some of the Windows 8–based devices of the future will offer decidedly lower-end feature sets, more similar to that of an iPad than a full-fledged Windows laptop. Even so, Microsoft specifies, among other things, that any logoed Windows 8 device must include at least 10GB of free storage space after Windows 8 completes the Windows Out Of Box Experience (OOBE); UEFI firmware (instead of BIOS); WLAN and Bluetooth 4.0 + LE (low energy) networking capabilities; graphics that are compliant with Direct3D 10 (but hardware acceleration is optional); 1366 × 768 or higher screen resolution; at least one 720p camera; an ambient light sensor; a magnetometer; a gyroscope; a 3-axis accelerometer; and stereo speakers (plus the five-point digitizer mentioned above).

Two-second resume. Much has been made about the requirement that all Windows 8 PCs be able to resume from Sleep in two seconds or less. However, less well known is the fact that this requirement doesn't apply to ARM-based Windows 8 devices, just those using the traditional Intel-based x86/x64 architecture. Rivera and I have a theory about this, which is that Microsoft simply doesn't have enough experience with power management on ARM yet to require this level of performance, but that such a requirement will be added in a future release, such as Windows 9.

Graphics driver updates can't require a reboot. Finally, Microsoft is requiring hardware makers to provide graphics device drivers that can be installed without requiring a system reboot. Previously, only Windows Display Driver Model (WDDM) drivers came with this requirement.

The Windows 8 Consumer Preview

Although Microsoft usually refers to its late February Windows 8 milestone as the Windows 8 Beta, Microsoft director of public relations Janelle Poole provided a new name for this release that I think more clearly reflects its purpose. She described it as the Windows 8 Consumer Preview, as opposed to the previous milestone, which was the Developer Preview.

I find this name interesting and telling, and I suspect that it will provide all of the end-user features that consumers expect. But this also suggests that the milestone after that, for now referred to as the Release Candidate (RC), might be aimed specifically at IT and the enterprise and thus could bear a name such as Business Preview. Regardless, the use of the word Consumer on the February release means to me that businesses will likely want to wait even longer before fully testing this OS release. And that means an even later deployment schedule than was previously thought.

This isn't a bad thing. Microsoft first told me over a year ago that it planned to make Windows 8 virtually identical to its predecessor for businesses and explained that from a deployment and management perspective, the OSs would behave very similarly. And from a user's perspective, Windows 8 can, of course, be controlled by policy to look and behave nearly identically to Windows 7, cutting down on training and support costs. Put simply, this is further evidence that Windows 8's stratospheric user experience changes could be aimed solely at consumers and that businesses won't need to worry about mixing and matching Windows 7 and Windows 8 in their environments.

So there you go: another month of Windows 8 information. Something tells me this is going to be pretty common throughout 2012. See you next month.

InstantDoc ID 141955

PAUL THURROTT (paul@windowsitpro.com) is the senior technical analyst for *Windows IT Pro*. He writes the SuperSite for Windows (winsupersite.com), a weekly editorial for Windows IT Pro UPDATE (www.windowsitpro.com/email), and a daily Windows news and information newsletter called WinInfo Daily UPDATE (www.wininformant.com).

Minasi

"Search-adaccount -accountinactive does a job that I've not seen other AD tools do as well."

Search-ADAccount and the Missing 15 Days

Time for more Active Directory cleaning!

Last month, in "Use Get-ADUser to Find Inactive AD Users" (InstantDoc ID 141486), I introduced *search-adaccount*, an AD cmdlet that can tell you which users' accounts are inactive (where "inactive" means the user hasn't logged on for some number of days). This month, I'll show you more of its syntax, as well as an interesting idiosyncrasy I call "the missing 15 days of *search-adaccount*."

To find out which accounts haven't logged on in, say, the past 90 or more days, you can type

```
search-adaccount -usersonly -accountinactive -timespan "90"
```

Note that you have to pass the "90" to *-timespan* with the double quotes, or it won't work as you expect and won't offer an error message, which leads to more troubleshooting than most of us want to experience. Another way to define "inactive" is to offer *search-adaccount* a particular date with the *-datetime* parameter. To see the users who haven't logged on since, say, December 1, 2011, you could type

```
search-adaccount -usersonly -accountinactive -datetime
  "1 December 2011"
```

Again, note that the date you pass to *-datetime* must be in quotes. As you learned last month, AD doesn't have an actual "inactive" flag in a user account, so *search-adaccount* determines whether an account is inactive with an AD attribute called *lastlogondate*. You can create a table of the inactive accounts by piping *search-adaccount* output to an *ft* (format table) command like so:

```
search-adaccount -usersonly -accountinactive -datetime
  "1 December 2011"|ft samaccountname,lastlogondate –auto
```

Try that command on a functioning, vibrant Active Directory (AD) domain, however, and play around with a number of different dates or time spans, and you'll start noticing something strange. If you had a user with a *lastlogondate* of, say, November 30, you'd expect a *search-adaccount* command with a *-datetime "1 December 2011"* parameter to catch that account (because November 30, 2011, occurs before December 1, 2011)—but it doesn't. In fact, that command won't report any users with a *lastlogondate* before approximately November 15. Similarly, if you were to do an equivalent command with the *-timespan* parameter, such as

```
search-adaccount -usersonly -accountinactive -timespan "29"
```

on December 30, 2011, you'd think that command would pick up everyone whose last logon date was December 1, 2011 (29 days prior to December 30) or earlier, but it doesn't. Instead, it reports only the folks with *lastlogondate* values around November 15 or earlier. It's as if *search-adaccount* includes a built-in 15-day grace period. What's up with that? I haven't talked to *search-adaccount*'s author, but my guess is that it's related to *lastlogondate*'s quirky nature.

You might recall that AD aims to update *lastlogondate* only once every 14 days, no matter how often you log on in that time period. Microsoft does that because every new value of *lastlogondate* kicks off some AD replication, and Microsoft fears that more frequent *lastlogondate* updates might burden your network. Thus, a *lastlogondate* of November 25, 2011, on a given user's account doesn't really mean that she last logged on November 25, 2011. More specifically, it means that this user's most recent logon might have happened on November 25, or she might have logged on a hundred times between then and December 9 (14 days after November 25), but AD just didn't update her *lastlogondate*—because it didn't have to. In light of that, you can see that it might be unfair to mark that user's account as inactive solely because of a *lastlogondate* of November 25, and that in truth "November 25" essentially equals "December 9" in this context. *Lastlogondate*'s "slop factor" is 14 days, so I imagine *search-adaccount*'s author added another day for good measure, and from that, *search-adaccount* got its 15-day grace period. It certainly seems a good compromise.

Some clients, however, haven't been happy to hear of this, because their legal and compliance folks want their lists of inactive users to reflect actual you-can-print-'em-out values of *lastlogondate*, and so they want *search-adaccount* to employ what might be called a strict interpretation of *lastlogondate*. For those folks, the answer is simple. If you want your inactive list to be close to *lastlogondate*'s actual value, subtract 15 from any *-timespan* values, and move any *-datetime* values 15 days into the future. Instead of *-timespan "90"*, use *-timespan "75"*; instead of *-datetime "1 December 2011"*, use *-datetime "16 December 2011"*.

Search-adaccount -accountinactive does a job that I've not seen other AD tools do as well. Next month, I'll show you a few more of its tricks!

InstantDoc ID 141849

MARK MINASI (www.minasi.com/gethelp) is a senior contributing editor for *Windows IT Pro*, an MCSE, and the author of 30 books, including *Mastering Windows Server 2008 R2* (Sybex). He writes and speaks around the world about Windows networking.

Otey

"SQL Server 2012's support for Windows Server Core enables leaner and more efficient SQL Server installations."

New Features in SQL Server 2012

Microsoft's enterprise data platform gets simpler licensing plus performance and development enhancements

The release of Microsoft SQL Server 2012 brings a host of important changes to Microsoft's enterprise data platform, including changes in the editions that Microsoft will offer as well as a new licensing model. SQL Server 2012 also introduces many performance, business intelligence (BI), and development enhancements. Here's a rundown of the top 10 new features in SQL Server 2012.

10 Simplified editions—SQL Server 2012 will be delivered in three main editions: Enterprise, Business Intelligence, and Standard. The Enterprise edition contains all of the product's features. The Business Intelligence edition contains all of the BI capabilities but lacks some higher-end availability features. The Standard edition provides basic relational, BI, and availability capabilities. Microsoft has retired the Datacenter, Workgroup, and Standard for Small Business editions but will continue to provide the Developer, Express, and Compact Editions.

9 Processor core licensing model—With SQL Server 2012, Microsoft has moved to a new core-based licensing model. The Enterprise edition can be licensed only per core. The list price is $6,874 per core. The Business Intelligence edition is licensed only per server; it goes for $8,592 per server. The Standard edition has the option of being licensed either per core or per server; it costs $1,793 per core or $898 per server.

8 Support for Server Core—Windows Server Core is designed for infrastructure applications such as SQL Server that provide back-end services but don't need a GUI on the same server. The inability to run previous versions of SQL Server on Server Core always seemed ironic. SQL Server 2012's support for Server Core enables leaner and more efficient SQL Server installations and reduces potential attack vectors and the need for patching.

7 Data Quality Services—Data Quality Services (DQS) is a knowledge-based tool that helps ensure your databases contain high-quality, correct data. DQS performs data cleansing, which can modify or remove incorrect data. It also does data matching to identify duplicate data and profiling that intelligently analyzes data from different sources.

6 T-SQL enhancements—SQL Server 2012 provides many T-SQL enhancements, including support for sequences, a new TRY_CONVERT operator for data conversions, OFFSET and FETCH for data paging, a new THROW operator for enhanced error handling, and improved T-SQL windowing functions.

5 Contained databases—Contained databases make it easy to deploy new databases and to move databases between SQL Server instances. Users don't need logins for the SQL Server instance; instead, all authentications are stored in the contained database. Contained databases have no configuration dependencies on the instance of SQL Server that they're hosted on.

4 Columnar index—The columnar index feature incorporates the same high-performance/high-compression technology that Microsoft uses in PowerPivot into the SQL Server relational database engine. Columnar indexes store data column-wise, and only the necessary columns are returned as query results. Microsoft states this technology can provide up to 10 times improvement in query performance with reduced I/O.

3 SQL Server Data Tools—One of the most important developer-oriented features in SQL Server 2012, SQL Server Data Tools uses the Visual Studio 2010 shell, and it enables model-driven database development as well as T-SQL and SQLCLR development and debugging. SQL Server Data Tools can connect to SQL Server 2005 and later as well as to SQL Azure.

2 Power View—Power View is a graphical data navigation and visualization tool that enables end-user reporting. Power View provides a report designer that lets users take elements from a semantic data model constructed by IT and use them to create powerful interactive reports that can be embedded in .NET applications or published to SharePoint.

1 AlwaysOn Availability Groups—The most important feature in SQL Server 2012 is the new AlwaysOn Availability Groups high-availability technology. AlwaysOn is essentially the evolution of database mirroring. It supports up to four replicas and lets you mix and match both synchronous and asynchronous connections. Unlike database mirroring, the data in the replicas can be actively queried.

InstantDoc ID 141978

MICHAEL OTEY (motey@windowsitpro.com) is senior technical director for *Windows IT Pro* and *SQL Server Pro* and author of *Microsoft SQL Server 2008 High Availability with Clustering & Database Mirroring* (McGraw-Hill).

Deuby

"Two sessions related to Active Directory at the recent Gartner Identity and Access Management Summit provide rich food for thought in the identity realm."

Identity Predictions

A report from the Gartner Identity and Access Management Summit

I recently attended the Gartner Identity and Access Management (IAM) Summit, sort of a three-day nerdvana for identity professionals. Though it's a relatively narrowly focused topic, identity permeates all aspects of modern computing, and this was reflected in the robust attendance; more than 800 attendees filled the halls of the conference center.

Even though the Gartner research firm hosts the conference and provides lots of one-on-one analyst time for its clients attending the conference, the conference isn't restricted to clients. As evidenced by the high blazer-to-beard ratio, however, it's a more upscale event than your average IT pro or security conference. (I also detected a slight yet disturbing increase in the number of Frank Zappa–like beards.) Gartner analysts have the luxury of interviewing many customers about their technologies, then going off and thinking about the data they've gathered—an amount of market research that most of us don't have time for. You might not agree with everything Gartner has to say, but it's as informed a viewpoint as anyone's out there. In this month's column, I'd like to review a couple of sessions that focused on Active Directory (AD)-related topics.

Despite AD's ubiquitous presence in the enterprise, Microsoft Forefront Identity Manager is the strategic IAM system for fewer than 15 percent of enterprises.

AD-Centric Universe

A session that naturally piqued my interest was *IAM in an Active Directory-Centric Universe* by Perry Carpenter and Andrew Walls. The first fact presented in the session got my attention: Despite AD's ubiquitous presence in the enterprise, Microsoft Forefront Identity Manager (FIM) is the strategic IAM system for fewer than 15 percent of enterprises. There's more activity around virtual directories nowadays than metadirectories. Carpenter and Walls agree with this; they say that virtual directories, such as Radiant Logic's RadiantOne Virtual Directory Server, are less complex to implement, they leave the data where it is in different repositories instead of bringing it all up to a metaverse, and they can offer better performance than a metadirectory service.

Regardless of how widely deployed FIM is, AD remains the 800-pound gorilla of enterprise identity stores. It's everywhere. As a result, any IAM solution—whether on premises or in the cloud—must be able to deal with AD securely and seamlessly. Because of AD's dominance in the enterprise authentication market, Carpenter and Walls stated that "Microsoft has a unique opportunity to shape the way identity will be managed and used in the next decade."

Although they're less talked about today, metadirectory services are still very much with us in the guise of the directory synchronization server. To explain, let me provide just a little bit of context. Last month, in "SCIM Simplifies Cloud Service Identity Provisioning" (InstantDoc ID 141564), I talked about the four A's of cloud identity: authentication, accounts, authorization, and auditing. *Accounts* describes account provisioning, the need to make user identities available to a cloud service so they can use the service. The directory sync server is one of several methods available today to accomplish this task. A synchronization server is (generally) an on-premises server that synchronizes users and groups between an enterprise IAM solution and a cloud service. The sync server monitors the content of, for example, an AD organizational unit (OU) or security group and keeps it in sync with the identity store of a cloud service. Users and groups are provisioned, or deprovisioned, from the service as they're added to the OU. Google Apps and Microsoft Office 365 are two prominent examples of Software as a Service (SaaS) applications that use directory-synchronization servers. Remember that, from the enterprise side, directory synchronization handles only account provisioning; you still must implement a federation solution with the SaaS provider to handle authentication of these accounts.

As technologists, we think of AD as a foundational piece of a company's IT infrastructure that provides integrated authentication and authorization for Windows computers (and more, if you buy extra bits). Microsoft marketers see AD, however, as glue (as evidenced by the term "AD-integrated") that ties other Microsoft products together in a way that makes them highly competitive against third-party solutions.

One result of this outlook is that AD enhancements that don't help sell other Microsoft products will take a back burner to enhancements that do. A great example is AD *bridge* products that allow UNIX and Linux computers to authenticate to an AD domain, thus simplifying the security environment. Microsoft has never expanded AD into this area, remaining content to allow third parties to add this capability. It's not hard to argue that time spent

developing this capability natively would offer little direct benefit to selling Microsoft products.

Another example is the movement to the cloud, where Microsoft is just another player in the market, rather than the dominant player. Microsoft provides Active Directory Federation Services (ADFS) for on-premises cloud identity, but enterprises are also looking at a new breed of identity applications (e.g., Identity as a Service—IDaaS) that hook in to AD to provide the same functionality. Gartner's position is that a complete IAM solution will always be a combination of native Microsoft applications, such as AD and perhaps AD FS for cloud identity or FIM for metadirectory and certificate services, and non-Microsoft apps such as AD bridges for UNIX clients, virtual directories for tying in other identity sources, privileged access management tools for governance, and lifecycle management tools to manage the digital identities themselves.

Puzzle Pieces

The second presentation I want to highlight, *Head in the Clouds: The Evolution of Directory Services* by Mark Diodati, provided a terrific overview of the bewildering complexity of ways that a directory service can be connected to a cloud service. Imagine a jigsaw puzzle in which the pieces are AD, on-premises identity provider federation services, cloud-based service provider federation services, IDaaS, virtual directories, directory synchronization servers, web applications . . . and don't forget the user in all this!

Then, attach these pieces to one another with the glue of Kerberos, SAML, federated trusts, proprietary vendor APIs, and different provisioning methods. The enterprise identity architect of the future (i.e., next week!) needs to understand how all these puzzle pieces can be arranged to accomplish an enterprise's cloud identity requirements.

And that's not all. These pieces all vary in the maturity of their solutions and their ability to integrate with one another. Authentication solutions are more mature than provisioning, and both have been around longer than governance.

Diodati groups these pieces into three broad categories—*to the cloud, in the cloud,* and *from the cloud*—then arranges them into typical use cases.

- *To the cloud* represents the use cases that we're most familiar with, that of enterprises with on-premises identity foundation (i.e., AD) that want to extend their identities to cloud applications using some kind of identity provisioning (e.g., directory sync) and an on-premises federation solution for authentication.
- *In the cloud* focuses on use cases for companies that have little or no on-premises IT infrastructure. These companies use IDaaS providers, such as Okta, that can have no on-premises components at all. The identity store is in the cloud, users authenticate to that cloud service, and once in, they use the service's built-in federation identity provider component to authenticate to the actual SaaS application.
- *From the cloud* describes the emerging use cases for companies that have their identities (or some portion thereof) in the cloud and want those identities provisioned down into on-premises applications. This is more or less the opposite configuration of *to the cloud* and is still very new and full of challenges. The first challenge, of course, is that few established companies today are willing to store their precious identity data in the cloud in the first place. A more likely use case is that of a company that already has a cloud service provider such as Google Apps as its authoritative identity source. If the company should eventually need an on-premises application, that company must get the identities down to the application using, for example, a virtual directory that presents them to the app via the LDAP interface the app expects.

According to Diodati, federation identity providers have become so common in the IAM arena that they're now just the "table stakes" a product must have to enter the market. Whether it's traditional all-in-one IAM solutions from CA or Oracle, dedicated on-premises cloud identity solutions from Ping Identity, virtual directory solutions, or IDaaS solutions, all now have a federated identity provider component. He believes the differentiator between these products is how directory-service and service-provider functions are beginning to work in both directions, so identity becomes another core IT function that's freed from the firewall.

In the end, Diodati had three straightforward recommendations. First, he joined the chorus of identity professionals recommending banishment of the password. (His exact words were, "Passwords suck!"—an observation right up there with Jeremy Grant's "We think the password needs to be shot.") To achieve this banishment, however, you must learn how to implement strong authentication methods (e.g., smart cards, hardware tokens).

Second, he said to accept the reality of directory synchronization. Though it's less technically elegant than just-in-time identity creation, service providers aren't going to depend on your off-premises identity for the health of their application. They want their own copy. What this makes me wonder, though, is how this will scale when a company uses hundreds or even thousands of SaaS providers? We'll need some kind of general-purpose sync engine that can handle many providers, not a dedicated server per provider.

Finally, he recommended that you track technological developments in this area, because they continue to evolve as cloud identity matures. You've gotten to the end of this column, so you get a gold star for effort on this recommendation!

What About You?

What do you think about these predictions? Are you using a metadirectory or a virtual directory to consolidate your identity sources—or are you using both? How are you progressing in the campaign to banish the password? You're the professionals who live with this day to day, so I'd really like to know your take.

InstantDoc ID 141861

SEAN DEUBY (sean@windowsitpro.com) is technical director for *Windows IT Pro* and *SQL Server Pro*, and former technical lead of Intel's core directory services team. He's been a directory services MVP since 2004.

READER TO READER

Fix for Double Vision in Disk Utilities

Bret A. Bennett

While researching a problem at Seagate's SeaTools forum, I ran across a post about disk drives showing up twice in the SeaTools disk diagnostic utility (forums.seagate.com/t5/SeaTools/Seatools-displays-the-same-drive-twice-in-the-display-screen/td-p/44805). The post presents a scenario in which the same disk drive is listed twice, yet the utility acts on only one instance of it. I've seen this "double vision" scenario before with another disk utility. Apparently, it's a common problem in disk utilities.

To fix the problem, open up Device Manager (devmgmt.msc) in Windows and select *Show hidden devices* on the View menu. In the devices tree, expand *Disk drives*. Notice that some of the icons are a light gray (i.e., grayed out), whereas others are a dark gray. Make sure you're able to differentiate between those that are grayed out and those that are the dark gray. You might need to run your display adapter's adjustment software or manually tweak your display monitor's settings to see the difference between the light and dark gray icons.

Some of the icons are grayed out because they're for removable drives that currently don't have anything inserted in them (e.g., drives for USB flash sticks). Some of the other grayed out icons will have the same name as disks you know are currently attached. Don't do anything to the dark gray icons. Instead, right-click the grayed out icons and select Uninstall. You'll get the message *Warning: You are about to uninstall this device from your system.* Click OK. (Note that it won't hurt anything to uninstall grayed out icons for items such as USB flash stick drives because the drives will be automatically reinstalled the next time you insert the devices into the computer.) Finally, run the disk utility again. You shouldn't have the same drive listed more than once this time around.

Based on my experience, drives become grayed out (i.e., orphaned) when the drives are removed and when disk controllers or disk controller drivers are changed. I've seen this happen when changing the BIOS Serial ATA (SATA) boot drive from IDE mode to Advanced Host Controller Interface (AHCI) mode. I've also seen this occur after running vendors' driver packages, such as the Intel Rapid Storage Technology Driver package and the older Intel Matrix Storage Manager Driver package.

Let's run through an example. I changed Windows 7's native SATA AHCI driver to Intel's ICH9R SATA driver. Figure 1 shows the *IDE ATA/ATAPI controllers* branch after this change. As you can see, uninstalling the Microsoft controller driver left five orphaned icons (i.e., ATA Channel 0 through ATA Channel 5). Note that you can still see the valid dark gray icons for ATA Channel 0 and ATA Channel 1. (This particular motherboard has two controllers.) Figure 2 shows the *IDE ATA/ATAPI controllers* branch after I "uninstalled" the five orphaned icons.

If you plan on uninstalling all the orphaned icons in the *Disk drives* and *IDE ATA/ATAPI controllers* branches of the devices tree as part of a spring cleaning mission, you might also want to do some spring cleaning in the tree's *Storage Volumes* and *Storage volume shadow copies* branches. However, you need to be very careful in the *Storage volume shadow copies* branch because each valid icon shows a light gray volume on top of a dark gray volume. The orphaned icons show a light gray volume on top of a light gray volume, as shown in Figure 3. The valid icon entries are created when a restore point is created. I'm not sure why the orphaned icons exist. Figure 4 shows the *Storage volume shadow copies* branch after I "uninstalled" the orphaned icons.

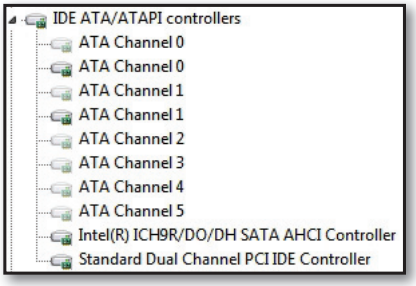


Figure 1: *IDE ATA/ATAPI controllers* branch containing orphaned icons

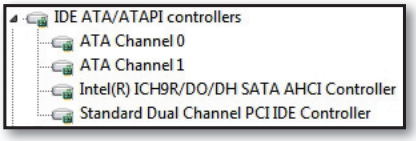


Figure 2: *IDE ATA/ATAPI controllers* branch after the orphaned icons were "uninstalled"

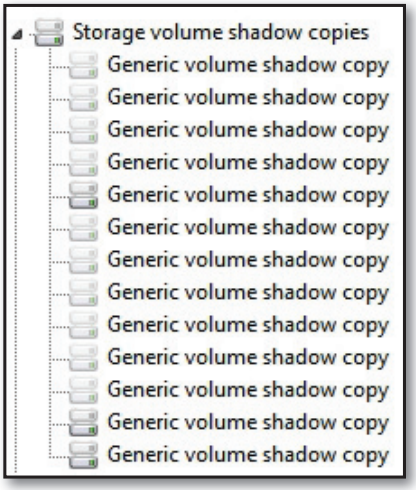


Figure 3: *Storage volume shadow copies* branch containing orphaned icons

Tell the IT community about the free tools you use, your solutions to problems, or the discoveries you've made. Email your contributions to r2r@windowsitpro.com.
If we print your submission, you'll get $100.

Submissions and listings are available online at www.windowsitpro.com. Enter the InstantDoc ID in the Search box.

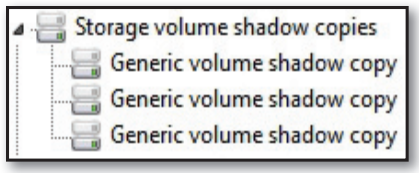


Figure 4: *Storage volume shadow copies* branch after the orphaned icons were "uninstalled"

I haven't experienced any noticeable performance increases or improved OS startup times by uninstalling orphaned icons. (However, I haven't clocked it to determine before and after statistics.) As far as I can tell, the cleanup simply removes the orphans from the disk utility software and releases registry space for reuse in the Windows System registry hive.

—Bret A. Bennett, IT consultant

InstantDoc ID 141851

Booting Windows 8 from a VHD in Windows 7

If you want to experiment with Windows 8 without having to sacrifice a physical system, you can boot Windows 8 from a Virtual Hard Disk (VHD) in Windows 7. Although you could use Hyper-V, I believe it's better to use real hardware to see how Windows 8 interacts with drivers. Here are the steps to boot Windows 8 from a VHD in Windows 7:

1. Make sure you have enough space (50GB to 60GB) on your hard disk.
2. In the Disk Management console in Windows 7, create a VHD. Format it as a fixed-size disk with 60GB.
3. Download the Windows 8 Developer Preview ISO file at msdn.microsoft.com/en-us/windows/apps/br229516.
4. Install Windows 8. At some point, you'll be prompted to select a hard disk for the installation. You want to install Windows 8 on the VHD, so do *not* select a hard disk. Instead, press Shift+F10 to go to a command-prompt window. At the command prompt, type DISKPART and press Enter. Then run the following commands:

```
DISKPART> select vdisk file=d:\VM\
  Win8.vhd
DISKPART> attach vdisk
```

5. Press Alt+Tab to go back to the disk selection window. Click refresh. You should see your new VHD listed. Select the VHD. You'll get an error message that states Windows can't be installed on this disk, but you can proceed with the installation.
6. Reboot when prompted to do so.

Chris Spanougakis

Windows 8 will automatically create an entry in the boot manager, so you don't have to use BCDEdit to add the entry, saving you a lot of work. As a result, after your machine reboots, you'll see the new boot loader. Click *Change defaults or choose other options* at the bottom of the screen to change the default OS that the computer will use to boot. You can also change some other options, such as the countdown timer for the selection of the OS and the device that the computer will use to boot.

—Chris Spanougakis

InstantDoc ID 141708

- Outlook
- Windows Event Log
- Hyper-V
- SQL Server
- VMware

ANSWERS TO YOUR QUESTIONS

Q: Why is there a performance problem between my Windows XP virtual machine running in Windows Virtual PC and my host computer?

A: Problems can be caused by your physical NIC using TCP offloading, and the emulated NIC within the virtual machine (VM) Intel 21140 not supporting TCP offloading. To address the performance problem between the VM and the guest, you have several options.

If you have multiple NICs in your desktop, you can disable TCP on the second NIC and use that NIC for the VMs. Another option is to disable TCP offloading on your system. To do so, navigate to HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\Tcpip\Parameters in the registry and create a DWORD value named DisableTaskOffload. Set it to a value of 1, then reboot.

—John Savill

InstantDoc ID 141835

Q: Can you use VMware Player to resolve application incompatibility problems in Windows 7?

A: Plenty of IT shops are considering making the move to Windows 7. Quite a few are already there. A big hurdle for some companies is the pool of mission-critical applications they're already using that aren't compatible with Windows 7. As a stopgap for the problem, Microsoft provides its no-cost Windows XP Mode add-on feature. This feature seamlessly presents applications in a Windows XP virtual machine (VM) into the user's Windows 7 desktop.

As an alternative to Microsoft's built-in solution, the no-cost VMware Player can also provide a similar experience by using its Unity feature. To enable the seamless presentation of an application, activate Unity mode by clicking VM, Enter Unity in VMware Player. Additional settings for Unity mode can be found in the properties screen for a VM. Select the Options tab, then Unity to configure how XP's windows are seen in Windows 7.

— Greg Shields

InstantDoc ID 141910

Q: Oracle products aren't supported on Hyper-V; does this mean they don't work on Hyper-V?

A: Not supported and not working are very different. Hyper-V is a great example: Many things that work on Hyper-V, such as running Windows 2000 in a virtual machine (VM), aren't supported by Microsoft. Microsoft doesn't support Win2K because it's no longer a supported OS.

It's very likely that Oracle products will run on Hyper-V (or any other hypervisor) without any problem. However, Oracle supports virtualizing its products only on its own hypervisor, Oracle VM. This is something you need to consider, because if you encounter a problem with an Oracle product on a non-supported hypervisor, you might have support challenges with Oracle. However, you might be willing to accept those challenges rather than run a separate hypervisor just for Oracle products. In my experience, and after conversations with customers, Oracle support does actually try and help with problems. They generally don't tell customers to reproduce the problem on Oracle VM, but be aware that they might.

—John Savill

InstantDoc ID 141824

Q: Can I restore a Virtual Hard Disk to a different Hyper-V server?

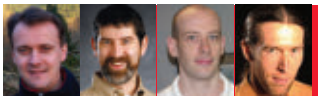
A: Yes, but not without the occasional hiccup. A Hyper-V Virtual Hard Disk (VHD) can be restored to an alternate server using any backup application. Hyper-V virtual machines (VMs) restored in this way might experience problems as they power on. Network adapter names might not be consistent with the new host, or machine configuration conflicts might exist in the VHD's saved state data.

To resolve a network adapter name inconsistency, launch the Hyper-V Management Console on the server where the VHD has been restored and open the Virtual Network Manager. Rename the restored VHD's network adapter to the same name as the adapter being used on the host. Then, start the VM.

If the VM still won't start, delete any saved state files by right-clicking the restored VM and selecting Delete Saved State. Occasionally, this step won't delete the necessary files. If not, locate the folder where the VHD has been restored and manually delete any existing .BIN or .VSV files.

— Greg Shields

InstantDoc ID 139636



Jan De Clercq | jan.declercq@hp.com
William Lefkovics | william@mojavemediagroup.com
John Savill | jsavill@windowsitpro.com
Greg Shields | virtualgreg@concentratedtech.com

Q: How can I improve responsiveness in low-bandwidth conditions for a Citrix XenDesktop VM?

A: Citrix's ICA protocol, with its added HDX extensions, supports a high-quality graphics experience for users, which operates well within a range of network conditions. When bandwidth between server and client gets too low, however, graphics responsiveness might no longer remain acceptable.

It's possible to improve responsiveness in such low-bandwidth conditions by enabling and configuring the Extra Color Compression and Extra Color Compression Threshold policies within the HDX Policies node of Citrix Desktop Studio. Be aware that enabling this compression results in lower-quality graphics.

— Greg Shields

InstantDoc ID 141529

Q: What are some simple tips for testing and troubleshooting Windows event forwarding and collection?

A: For testing Windows event forwarding and collection, you can use the Eventcreate command-line utility (eventcreate.exe). This tool lets an administrator create a custom event in a specified event log. For example, to create an event with event ID 100 in the application log, you can type the following command on the event source computer:

```
eventcreate /t error /id 100
  /l application /d
  "Custom event in application log"
```

If all event forwarding and collection components are functioning properly and there's normal network latency, the test event you create on a source computer should arrive in the event collector's Forwarded Events log within one minute. If the event doesn't appear on the event collector, consider the following simple troubleshooting steps.

Check Group Policy Object settings. Check that you've applied the latest Group Policy Object (GPO) settings on the source computer. The configuration for event forwarding on the source computer can be set using GPO settings. To make sure the latest GPO settings have been applied, you can force GPO application by typing the following at the command line on the source computer:

```
gpupdate /force
```

Check Windows Remote Management. Check the status of the Windows Remote Management (WinRM) service on the source computer. Make sure WinRM is running and set to start automatically. On Windows clients, WinRM isn't enabled and configured by default, but you can easily do so from the command line using the winrm command and the quickconfig switch, as follows:

```
winrm quickconfig
```

This command sets the WinRM service to start automatically, creates a WinRM listener, and creates a Windows Firewall exception for WinRM.

Check the event collector. Make sure that the event collector can reach the source computer using WinRM. To do so, run the following command on the event collector:

```
winrm id -remote:<source_computer_name>
   -auth:none
```

If you use collector-initiated event subscriptions, make sure the collector is using the correct credentials for connecting to the source computer. To check the credentials against the source computer, run the following command on the collector machine:

```
winrm id -remote:<source_computer_name>
   -u:<username> -p:<password>
```

If you use collector-initiated event subscriptions, check that the user name you use to connect to the source computer is a member of the Event Log Readers group on the source computer. This is a predefined local group that controls access to the local event logs. Only members of a computer's Event Log Readers group can read the events on that particular computer.

Check the source computer. Has it registered with the event collector? To list all registered source computers for a given subscription, use the following Windows Event Collector Utility (wecutil.exe) command:

```
wecutil gr <name_of_subscription>
```

Check that event forwarding isn't blocked. Make sure that event forwarding isn't blocked on the event collector due to incorrect Windows Firewall configuration settings. The Windows Firewall Inbound Rules should be enabled for accepting these incoming WinRM connections: Windows Remote Management (HTTP-In) and Windows Remote Management Compatibility Mode (HTTP-In). If you've configured a subscription to use the HTTPS protocol, you must also make sure that you create a Windows Firewall exception for HTTPS on port 443.

You can find more troubleshooting tips for event forwarding and collection in the Microsoft TechNet article "Configure Computers to Forward and Collect Events" (technet.microsoft.com/en-us/library/cc748890.aspx).

—Jan De Clercq

InstantDoc ID 141699

Q: When creating a new rule in Microsoft Outlook 2010 or Outlook 2007, what happens if I apply the rule to messages already in the folder?

A: I sometimes create new Outlook rules on the fly while reviewing email messages. Outlook makes this process simple with a button in the Ribbon of an open message. In Outlook 2007, you select Create Rule in the Actions tab of an open message. In Outlook 2010, Create Rule is found in the drop-down menu of the Rules button. Outlook offers simple rule creation with common message properties through this method. You can select Advanced at the bottom of the Create Rule dialog box to show all of the options for new rule creation in the Rules Wizard. A common rule I see is the simple act of moving a message to a subfolder based on sender or subject.

When you create such a rule in Outlook, you're presented with the option of applying the rule to messages already

received. Outlook searches your Inbox (or whatever folder you launched this message from), checking for items that match the parameters you set in the rule. If you have a lot of messages in the folder, typically your Inbox, this action can take some time. Of course, this functionality is powerful, requiring no effort from the user except that of patience. However, you won't be able to access anything else in Outlook while it searches mail folders for items that apply to your newly created rule.

If you have a significant number of messages stored in your Inbox, Outlook can take minutes to apply the rule against every message therein. If the folder you're searching is a local .pst file, it might take even longer. I found that with 1,000 messages in a .pst folder, it was faster to manually sort the messages by Subject (or Sender, or whichever parameter you used in the rule), then drag and drop the content to the intended subfolder.

When I tested a rule on a .pst folder with 25,000 messages, Outlook took four minutes to finish. Sometimes, it's just easier to do things yourself, especially if you're as impatient as I am.

—William Lefkovics

InstantDoc ID 141748

Q: My Microsoft SQL Server database shows a very large size, but the sum size of all the tables is nowhere near the size of the database. What should I do?

A: The first step to try is to shrink the database, which is done through SQL Server Management Studio (SSMS). Right-click the database and select Tasks, Shrink, Database (see Figure 1). You can accept the default options and click OK to perform the shrink operation (see Figure 2).

If this doesn't help, then jump to Explorer and look at the file system. The most likely problem is that you have a very large transaction log file that's never shrinking because you don't make backups. This could be a huge problem if this is production data.

When you created the database, you specified a location for the database and a location for the transaction log. These are normally different drives, to avoid the chance of a physical disk problem affecting both your database and transaction logs. If you didn't set a custom location, the database files and transaction logs will be in the same location, which is C:\Program Files\Microsoft SQL Server\MSSQL10.MSSQLSERVER\MSSQL\DATA for SQL Server 2008 R2. If you're unsure of the location, right-click a database within SSMS and select Properties, and in the Files section you should see the exact path of the log and database, which Figure 3 shows.

In my example, I looked at the files and noticed that although I had a 90MB database for ReportServer, I had a 24GB transaction log file, which Figure 4 shows. This is because I never performed a backup of the database, which would have cleaned up the transaction file.

To fix this problem, I needed to perform a backup. However, I didn't want to perform an actual backup, so I backed up to a null device. Then I performed a shrink on the log file. I ran these commands in a query window within SSMS:

```
backup database ReportServer to disk
  = 'nul:'
backup log ReportServer to disk
  ='nul:'
```

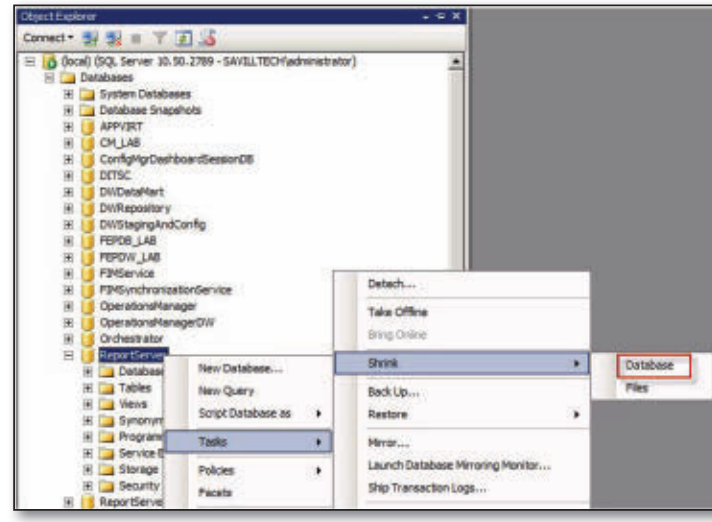


Figure 1: Shrinking a database

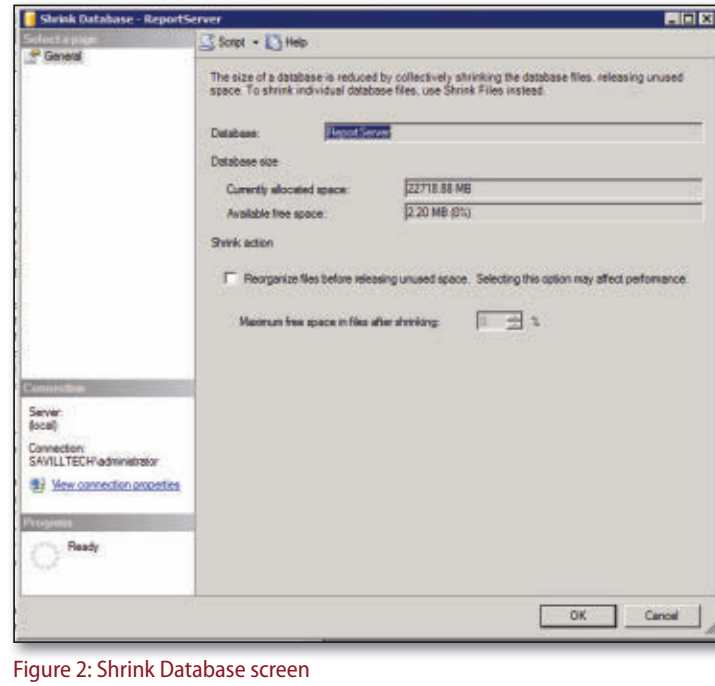


Figure 2: Shrink Database screen

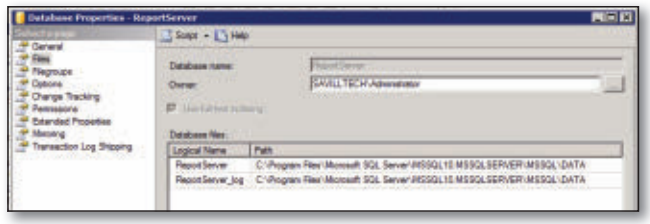


Figure 3: Exact path of a log and database

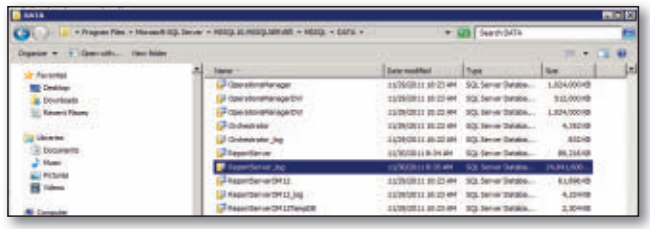


Figure 4: Example of a large transaction log file

Figure 5: Improved transaction log file

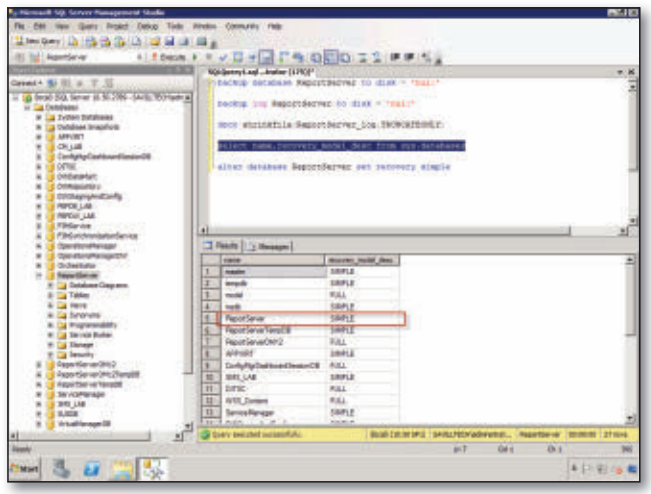


Figure 6: Checking whether changing recovery mode worked

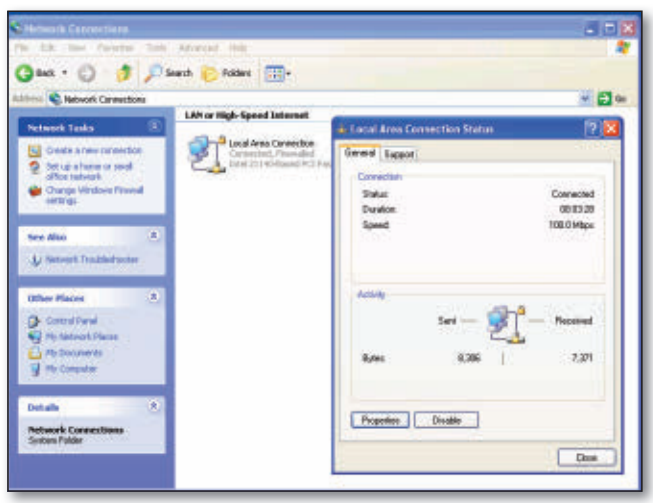


Figure 7: Properties window showing speed of VM connection

```
dbcc shrinkfile(ReportServer_
  log,TRUNCATEONLY)
```

I then looked at my files again. The transaction log was now 4MB, which was much better (see Figure 5). To avoid this problem in the future, since I don't intend to back up this database, I can change the recovery mode of my database from Full to Simple. This means the transaction logs will automatically truncate at checkpoint times, which are performed automatically. To look at the current recovery mode, run this command:

```
select name,recovery_model_desc from
  sys.databases
```

To change the recovery mode of the database to Simple, use this command:

```
alter database ReportServer set
  recovery simple
```

To check whether the change took effect, you would re-run the select recovery_model command I mentioned earlier. You would then see the type as SIMPLE, which Figure 6 shows.

—John Savill

InstantDoc ID 141833

Q: I'm using Windows Virtual PC with Windows 7. How can I update the device driver to match the real NIC?

A: If you open Network Connections within the Windows XP virtual machine (VM) and double-click the Local Area Connection, the properties open and show you a speed of 100Mbps, as Figure 7 shows. It's important to remember that this is a VM, and it sees emulated hardware.

In this case, Windows Virtual PC provides an emulated Intel 21140 Ethernet device that runs at 100Mbps, so that's the speed that's always seen, regardless of the true speed of the connected physical NIC. Note, however, that this 100Mbps is just a label. In reality, the virtual NIC operates at the same speed that's capable of the true physical NIC.

—John Savill

InstantDoc ID 141834

Avoid Active Directory Mistakes in Windows Server 2008

Don't let these Adprep and Dcpromo errors take you by surprise

by Justin Hall

When customers install Microsoft Active Directory Domain Services (AD DS) in Windows Server 2008 or Server 2008 R2, a couple of issues sometimes come up. One issue involves installation; another is about Microsoft's recommendations for running domain controllers (DCs) as virtual machines (VMs).

These issues might be familiar to experienced administrators. But if you're a less-experienced administrator who needs to replace DCs that run Windows Server 2003 with those that run Server 2008 R2, this article will shed some light on these issues and can help you avoid problems.

Adprep-Related Errors

Adprep is a utility that you run to prepare an existing Active Directory (AD) environment for the first DC that runs a newer OS, such as Server 2008 R2. If you have an AD environment in which all DCs run Server 2008 or Windows 2003, and you want to add the first DC that runs Server 2008 R2, then you need to run certain Adprep commands:

1. Run adprep /forestprep on the schema master.
2. Run adprep /domainprep on each domain's infrastructure master.
3. If you plan to install a read-only DC (RODC—new in Server 2008), then you also need to run adprep /rodcprep for every domain that will have an RODC.

The article "The Adprep Process" (www.windowsitpro.com/article/domains2/the-adprep-process) tells more about this process, which is straightforward enough. Still, administrators often have questions:

- What exactly does Adprep do?
- What is the process for making sure that any necessary Adprep commands run successfully?
- How do I work around any errors?

The Microsoft article "Running Adprep.exe" (technet.microsoft.com/en-us/library/dd464018%28WS.10%29.aspx) explains all that and more: the utility's general purpose, the process for running the necessary commands, and how to validate the utility's success. (If you want to review the exact changes that Adprep operations make to prepare an existing AD, see the Microsoft articles "Windows Server 2008: Appendix of Changes to Adprep.exe to Support AD DS" at technet.microsoft.com/en-us/library/cc770703%28WS.10%29.aspx and "Windows Server 2008 R2: Appendix of Changes to Adprep.exe to Support AD DS" at technet.microsoft.com/en-us/library/dd378876%28WS.10%29.aspx.)

An Adprep Caveat

When the requirement to run the adprep /forestprep command was originally introduced in Windows Server 2003, Microsoft and some partners recommended taking the precaution of isolating the Schema Master (e.g., temporarily placing it on a separate network) to better control the schema update process. Since then, Microsoft Customer Service and Support (CSS) has seen this approach cause more problems than it potentially solves for most organizations. As a result, Microsoft no longer recommends taking the Schema Master offline before you run adprep /forestprep.

InstantDoc ID 142163

When running Adprep, plan for these important factors:

- Credentials—Prepare to specify the necessary credentials for each Adprep command. Depending on the command, you might need to supply credentials for an account that is a member of the Schema Admins, Enterprise Admins, or Domain Admins group.
- Access to Flexible Single-Master Operation roles (FSMOs)—You need to run Adprep on the Schema Master of the forest and on the Infrastructure Master in the domain in which you're installing the new DC. Note that you need either to run the command from the new OS DVD on the Operations Master, or to copy the Adprep utility and its folder contents from the DVD before running it. (See the sidebar "An Adprep Caveat" for a warning about isolating the Schema Master.) Be aware that Server 2008 R2 includes both 32- and 64-bit versions of Adprep (in the \support\adprep folder of the OS disk). The 64-bit version runs by default. If you're running Adprep on a 32-bit system, be sure to use Adprep32.exe instead.
- Replication—Make sure that replication is working throughout the forest. Take a look at "Troubleshooting Active Directory Replication" (www.windowsitpro.com/article/active-directory/troubleshooting-active-directory-replication) and "Active Directory Replication In Depth" (www.windowsitpro.com/article/active-directory/gain-a-better-understanding-of-exactly-how-active-directory-replication-works-135815) for more information about troubleshooting AD replication.

If you can prepare for these potential issues and follow the process that the previously mentioned articles describe, you should have no trouble. In some cases, though, you might see one of these errors during an Adprep operation:

- Rodcprep fails if the DNS partition's Infrastructure Master is assigned to a demoted or invalid FSMO owner. Each application directory partition in a forest has an Infrastructure Master, and the Rodcprep command contacts each one. Rodcprep fails if the Infrastructure Master is assigned to a deleted DC. For example, you might have forced the demotion of a DC without realizing that it was assigned the Infrastructure Master role of an application partition, until you see this error when you run Rodcprep. The Microsoft article "Error message when you run the 'Adprep /rodcprep' command in Windows Server 2008: 'Adprep could not contact a replica for partition DC=DomainDnsZones,DC=Contoso,DC=com'" (support.microsoft.com/kb/949257) includes a script to resolve this error.
- An error, "An attribute with the same link identifier already exists," might occur when you run the adprep/forestprep command on a Windows 2003 computer. You see this error if the adprep /forestprep command tries to add a new object to the schema partition by using a link ID that has already been assigned to an existing object in that partition. The Microsoft article "An error occurs when you run the ADPREP/FORESTPREP command on a Windows Server 2003-based computer: 'An attribute with the same link identifier already exists'" (support.microsoft.com/kb/969307) explains how to solve this issue.

The overall Server 2008 or Server 2008 R2 upgrade process is described in the Microsoft article "Upgrade Domain Controllers: Microsoft Support Quick Start for Adding Windows Server 2008 or Windows Server 2008 R2 Domain Controllers to Existing Domains" at technet.microsoft.com/en-us/library/upgrade-domain-controllers-to-windows-server-2008-r2(WS.10).aspx.

DNS Delegation Error

After Adprep completes successfully, you can install the first DC that runs Server 2008 or Server 2008 R2 into your existing AD. If you choose to install the DNS server role during the DC installation, you might see this warning, which Figure 1 shows: "A delegation for this DNS server cannot be created because the authoritative parent zone cannot be found or it does not run Windows DNS server. If you are integrating

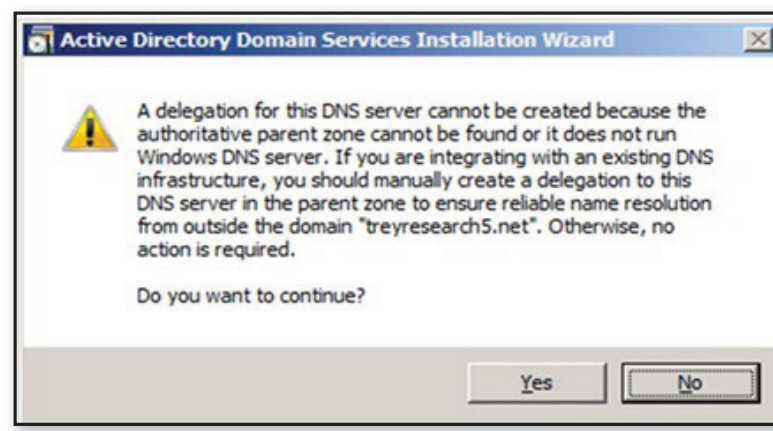


Figure 1: DNS delegation error

with an existing DNS infrastructure, you should manually create a delegation to this DNS server in the parent zone to ensure reliable name resolution from outside the domain 'treyresearch5.net.' Otherwise, no action is required."

Before Server 2008, many customer problems with AD installations were caused by underlying problems with the DNS infrastructure, such as missing or incorrect DNS delegation records. One of Microsoft's goals for improving AD DS installation in Server 2008 was to help customers initially configure the correct DNS infrastructure and then to help them maintain that configuration.

To that end, the AD DS installation wizard (Dcpromo) in Server 2008 and later automatically tries to create a DNS delegation when you create a new forest. The DNS delegation helps to ensure that clients from other domains can resolve host names in the domain of the new DC. If you aren't concerned about the ability of people in other domains or on the Internet to resolve DNS name queries for computer names in the local domain, you can disregard the message that Dcpromo uses to create this DNS delegation; simply click Yes when the message appears.

The message appears when these three conditions are met:

- Dcpromo has been configured to install the DNS server role.
- Too few delegations exist between DNS servers in the immediate parent DNS zone and the subdomain in which you're installing the new DC.
- The DC that you're installing cannot create a delegation to the DNS subdomain on a DNS server that is authoritative for the parent zone.

Dcpromo tries to create the delegation to ensure that computers in other domains can resolve DNS queries for hosts, including DCs and member computers, in the DNS subdomain. Dcpromo can automatically create such delegations only on Microsoft DNS servers; the effort will fail if the parent DNS domain zone resides on third-party DNS servers such as BIND.

You can see this error when you install DCs in forest root domains that have two- or three-part names (such as contoso.com or corp.contoso.com) and that are immediately subordinate to top-level Internet domains such as .com, .gov, .biz, .edu, or two-letter country code domains such as .nz and .au. If your AD domain is to be registered on the Internet by the time it is promoted, the logging of this error might indicate that your ISP or DNS hosting provider hasn't yet created the necessary delegation to your AD subdomain.

You might also encounter this error when creating DCs in a forest root domain that is subordinate to an existing corporate intranet namespace. For example, if BIND DNS servers own the internal domain contoso.com, then you'll encounter this error when Dcpromo attempts to create the delegation from contoso.com to the AD forest root domain's corp.contoso.com subdomain.

For Dcpromo to create the delegation on authoritative DNS servers in the parent domain, these conditions must be met:

- The parent DNS server must run the Microsoft DNS Server service.

Only supported backup solutions, such as Windows Server Backup, can be used to restore a DC.

- The Microsoft DNS server in the parent domain must be online and accessible over the network from the DC that you're installing.
- The user running Dcpromo on the DC that you're installing must have Domain Admins, Enterprise Admins, or DNS Admin credentials in the parent DNS zone.

Given that many AD domains aren't registered with an Internet registrar, and that the DNS servers for top-level domains (TLDs) run BIND, you can safely ignore this error message and click Yes to continue the promotion.

When delegations should exist between the parent domain and the subdomain that's being promoted, you can create and validate those delegations before or after the Dcpromo promotion. There's no reason to delay the promotion of a new DC that presents this error. To avoid the error message in future Dcpromo promotions, take one of these actions:

- Pre-create the delegation on third-party DNS servers in the immediate parent domain.
- Make sure that DCs that are being promoted have network connectivity and the necessary administrative credentials to create delegations on Microsoft DNS servers that host the parent DNS zone.
- Specify the /CreateDNSDelegation:No argument in the Dcpromo command line or answer file.

For more information about DNS delegation, see the Microsoft article "Understanding Zone Delegation" (technet.microsoft.com/en-us/library/cc771640.aspx). If zone delegation isn't possible in your situation, you might consider other methods for providing name resolution from other domains to the hosts in your domain. For example, the DNS administrator of another domain could configure conditional forwarding, stub zones, or secondary zones to resolve names in your domain. These Microsoft articles explain these concepts in more detail:

- "Understanding Zone Types" (go.microsoft.com/fwlink/?linkid=157399)
- "Understanding stub zones" (go.microsoft.com/fwlink/?linkid=164776)
- "Understanding forwarders" (go.microsoft.com/fwlink/?linkid=164778)

Virtual DCs and Update Sequence Number Rollback

Although Microsoft has published guidance and best practices for running DCs as VMs (see "Running Domain Controllers in Hyper-V" at technet.microsoft.com/en-us/library/virtual_active_directory_domain_controller_virtualization_hyperv%28WS.10%29.aspx), some customers who run virtual DCs have problems with update sequence number (USN) rollback. The problems are often caused by improper restores of the VM. For example, replication errors appear and are determined to be caused by a USN rollback, which was the result of a restored snapshot of the virtual DC.

Only supported backup solutions, such as Windows Server Backup, can be used to

```
dcpromoui Enter ComposeFailureMessage
dcpromoui Enter GetErrorMessage 80070524
dcpromoui Enter State::GetOperationResultsMessage The attempt
  to join this computer to the <target DNS domain> domain
  failed.
dcpromoui Enter State::GetOperationResultsFlags 0x0
dcpromoui Enter State::SetFailureMessage The operation failed
  because:
The attempt to join this computer to the <target DNS domain>
  domain failed.
"The specified user already exists."
```

Figure 2: Error text in the dcpromoui.log file

```
A dcpromoui Enter DS::JoinDomain

  dcpromoui Enter MassageUserName administrator
  dcpromoui z.com\administrator
B dcpromoui Enter MyNetJoinDomain contoso.com\DC1.contoso.com

  dcpromoui Calling NetJoinDomain
  dcpromoui lpServer : (null)
  dcpromoui lpDomain : contoso.com\DC1.contoso.com
  dcpromoui lpAccountOU : (null)
  dcpromoui lpAccount : contoso.com\administrator
  dcpromoui fJoinOptions : 0x27
  dcpromoui HRESULT = 0x80070524
```

Figure 3: Searching dcpromoui.log for the helper DC name

restore a DC. Microsoft has recently revised the recommendations for running DCs as VMs, specifically the explanation of USNs and how to prevent USN rollback. These revisions should make the information more concise and clear and help customers avoid problems.

"The Specified User Already Exists" Error

In some cases, AD installation on a workgroup server might fail and return this error on the Summary page: "The operation failed because: The attempt to join this computer to the <target domain> failed. 'The specified user already exists.'" In this situation, the dcpromoui.log file, which is stored in the \%windir%\debug folder, contains the text that Figure 2 shows.

This error most often indicates that the server you're promoting has the same host name as another DC. Follow these steps to fix the issue:

1. If you're replacing a previously demoted DC with a new DC of the same name, make sure to remove the old DC's metadata. In Server 2008 and later, AD snap-ins provide a simplified way to remove DC metadata. If necessary, you can also use the legacy method: Ntdsutil.
2. If Dcpromo continues to fail with this error, review the dcpromoui.log file to identify the name of the source DC (aka the helper DC) that the new replica DC is using for replication. Search the file for the section that begins at callout A in Figure 3. The name of the source DC appears in the output at callout B.
3. Verify that the source DC has inbound replicated the removal of the DC metadata (i.e., the conflicting DC machine account and NTDS Settings objects). If the DC machine account still exists, then determine the reason:
   - simple replication latency, such as a DC that is several hops away from the DC that originated the metadata-cleanup operation
   - an inbound replication failure on the helper DC or on the source DC from which the helper DC receives changes
   - a helper DC in a "lag site" that has been intentionally configured to inbound replicate changes to AD in a delayed fashion

The error can have other root causes aside from a conflicting machine account. These Microsoft articles discuss these other possible causes:

- "'Computer <name> is already in use' error message when you add user names in Windows 2000 or Windows Server 2003" (support.microsoft.com/kb/266633)
- "Error Message 'lsass.exe-System Error' After Running the Dcpromo.exe Program" (support.microsoft.com/kb/273875)
- "You cannot add a user name or an object name that only differs by a character with a diacritic mark" (support.microsoft.com/kb/938447)

Sometimes Dcpromo fails while trying to create the NTDS Settings object for the DC. In this case, several errors might display a similar message; the extended error information will help to identify the root cause. Look for text such as "The operation failed because . . ." or "Active Directory could not create the NTDS Settings object . . ."

For example, Dcpromo can fail with this on-screen error: "The operation failed because: Active Directory could not create the NTDS Settings object for this domain controller <NTDS Settings

Figure 4: Access denied error

Table 1: Possible Extended Error Strings

Error String	Decimal Error	Hexadecimal Error	Resolution
Access is denied	5	5	Check system time, including YY, MM, DD, AM/PM + Time zone, for accuracy between the new replica, Key Distribution Center (KDC), and helper DC. Correct the time as necessary, reboot the DC that's being promoted, and retry the operation. Also verify user rights assignment.
An attempt was made to add an object to the directory with a name that is already in use	8305	0x2071	See the Microsoft article "Error message when you re-install ISA Server 2004 and CSS on a computer that is a member of an ISA Server array" (support.microsoft.com/kb/925883).
Could not find the domain controller for this domain	1908	0x774	KDC is disabled. Verify that the KDC service status is Running and that the service startup value is Automatic. Reboot with the correct configuration. (See the Microsoft article "How to force Kerberos to use TCP instead of UDP in Windows" at support.microsoft.com/kb/244474.)
The Directory Service cannot perform the requested operation because a domain rename operation is in progress	N/A	N/A	This issue can be caused by a recently completed or in-progress domain rename operation. (See the Microsoft article "Error message when you use the Active Directory Installation Wizard to add a member server in a Windows Server 2003 SP1 domain" at support.microsoft.com/kb/936918.)

Table 2: GPMC and Gpresult Settings

Setting	Security Principals
Access this computer from the network (enabled by default in Default Domain Controllers Policy)	Must include • Administrators • Enterprise Domain Controllers • Authenticated Users
Deny access to this computer from network (not defined by default in Default Domain Controllers Policy)	If enabled, must not include • Enterprise Domain Controllers • Everyone • Administrators • Authenticated Users

object DN path> on the remote domain controller <fully qualified computer name of source DC>. Ensure the provided network credentials have sufficient permissions. <%Extended error string%>." Be aware that the boilerplate text "Ensure the provided network credentials have sufficient permissions" can be misleading; the failure to create the NTDS Settings object isn't necessarily caused by insufficient credentials. Table 1 lists possible extended error strings for this error message.

Another common cause of AD installation failure is not granting the Administrators group the *Enable computer and user accounts to be trusted for delegation* user right. This right is a Group Policy setting that is enabled for the Administrators group by default in the Default Domain Controllers Policy.

When a DC is selected as a replication partner during the promotion of a replica DC, the selected DC requires access to resources on the computer that you're promoting. If the *Enable computer and user accounts to be trusted for delegation* user right is not granted to the Administrators security group, then each access request for a resource fails with the "access denied" error that Figure 4 shows.

To resolve the error, use Group Policy Management Console (GPMC) and the Group Policy Results tool (Gpresult) to verify that the Administrators group is granted the *Enable computer and user accounts to be trusted for delegation* user right in the Default Domain Controllers Policy. The path in Group Policy Editor is \Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment\Enable computer and user accounts to be trusted for delegation.

After a DC is running Server 2008 R2, you can run the AD DS Best Practices Analyzer (BPA) to catch this kind of policy-setting misconfiguration. The appropriate BPA rule isn't included in the original set of rules but is part of a supplementary set of rules that's delivered via Windows Update. This rule will be applied to a DC that runs Server 2008 R2.

When you run the AD DS BPA, another rule from the same supplementary set can help prevent a couple of common Group Policy setting misconfigurations that are root causes of DC replication failure: not granting the *Access this computer from the network* user right to the Administrators, Enterprise Domain Controllers, or Authenticated Users security groups, or having the Enterprise Domain Controllers, Everyone, Administrators, or Authenticated Users security groups in the settings of the *Deny access to this computer from network* user right. Any DC that tries to replicate from a DC with one of the aforementioned policy settings might fail. Users and computers might also experience failure to apply Group Policy Objects (GPOs).

To resolve that error, follow the steps in the BPA to verify that the DCs have this user right granted to the appropriate security principals. You can use the GPMC and Gpresult settings in Table 2 to verify that Group Policy reflects the correct settings.

Better Troubleshooting

The good news is that the new Windows PowerShell cmdlets for AD DS installation and replication management in Windows Server 8 address these issues. In the meantime, explaining these issues will hopefully help administrators who need to install and troubleshoot DCs that run Server 2008 R2 to be better informed and less hindered.

InstantDoc ID 142023

Justin Hall
(justinha@microsoft.com) is a senior technical writer at Microsoft. He has written and edited articles about Active Directory since 2001.

Quick Reference Guide: ACTIVE DIRECTORY AUDITING

Active Directory Auditing Configuration Checklist:

- [ ] Audit Policy settings configured in GPO.
- [ ] Object-Level AD auditing settings configured.
- [ ] Event log settings set.
- [ ] For fully automated AD auditing try NetWrix AD Change Reporter: ***www.netwrix.com/ADAref***

How To #1: Audit Policy Settings

Using the Group Policy Management Console, edit ***"Default Domain Controllers Policy"***:

Computer Configuration > Policies > Security Settings > Local Policies > **Audit Policy** > **Audit Account Management** > Define > **Success** > **Audit directory service access** > Define > **Success** > Computer Configuration > Policies > Security Settings > Local Policies > **User Rights Assignment** > **Manage auditing and security log** > Define > Add User/Group (Default=Administrators)

How To #2: Object-level AD Auditing

Launch ADSIEdit from Administrator Tools > Right-click Domain > Properties > Security (Tab) > Advanced (Button) > Auditing (Tab) > Select "Everyone" > Edit (Button) > Make sure the following are **OFF:**

- Full Control, List Contents, Read all properties, Read permissions

> Select "Apply these auditing entries to objects and/or containers within this container only" (Check Box) > Click "OK" x3

How To #3: Security Event Log Settings

Perform the following using GPMC, edit ***"Default Domain Controllers Policy"***:

> Computer Configuration > Policies > Security Settings > Local Policies > **Event Log** > **Maximum security log size** > Define > 130048 > OK

> **Retain security log** > Define >14* > OK

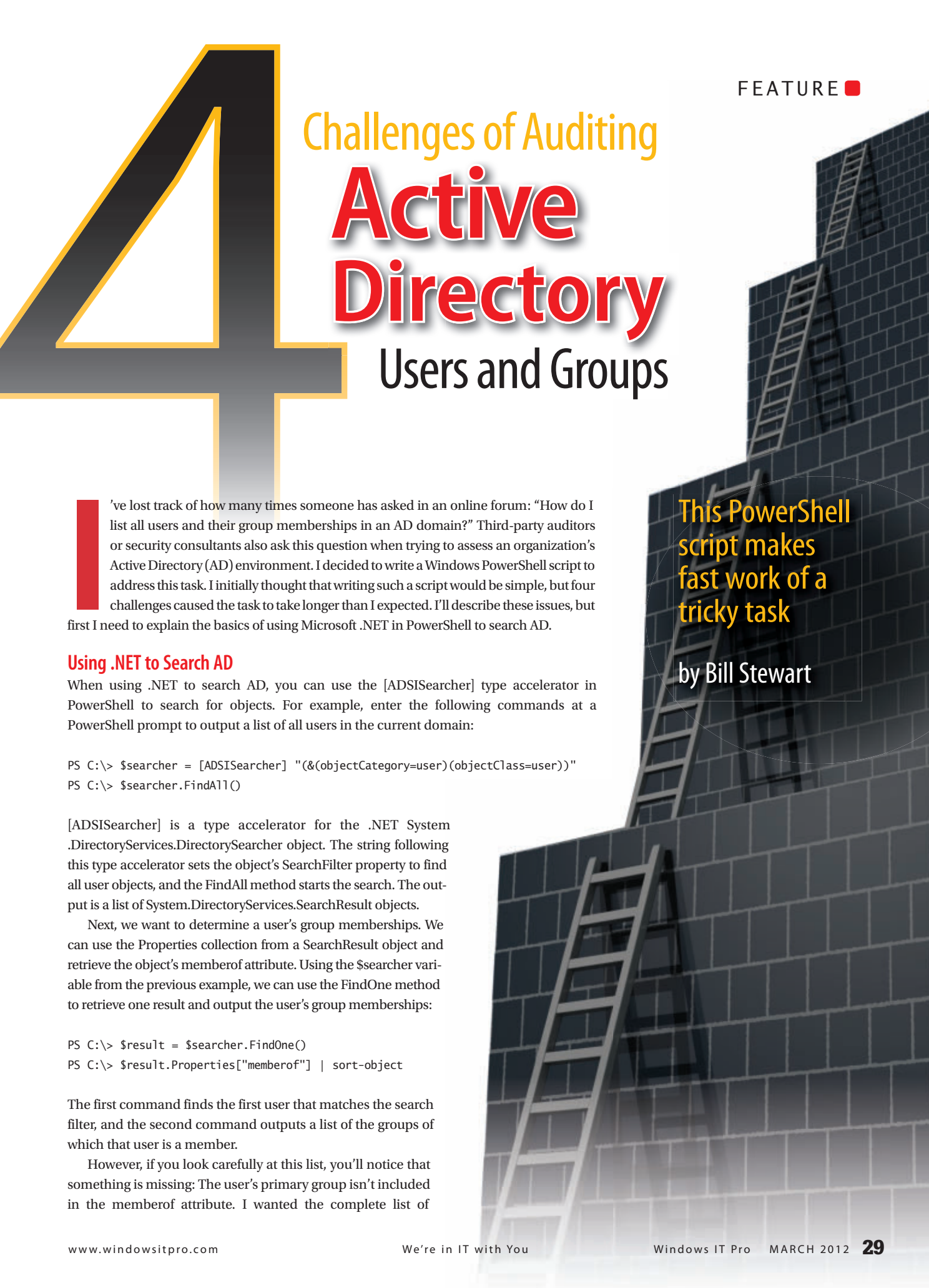
> **Retention method for security log** > Define > Overwrite events **as needed**

**Check available disk space*

Event ID Reference (2K3/2K8)

517/1102 – Security Log Cleared
528/4624 – Login Succeeded
529/4625* – Failed Login
530/4625* - Failed Login (Time Restr.)
531/4625* – Disabled User Acct.
532/4625* – Account Expired
533/4625* - Failed Login (Wrkst. Restr.)
534/4625*(5461) - Failed Login (Does not have rights to use login method)
535/4625* – Password Expired
539/4625* – Failed Login, Acct. Locked
540/4624 – Login Succeeded (2k, k3, xp)
624/4720 – User Acct. Created
626/4722 – User Acct. Enabled
628/4724 – User Acct. Password Set
629/4725 – User Acct. Disabled
630/4726 – User Acct. Deleted
63(1), (5), 648, 65(3), (8), 663/
47(27), (31), (44), (49), (54), (59)
Group Created
632, 636, 650, 655, 660, 665/4728, 4732, 4746, 4751, 4756, 4761
Group Member Added
633, 638, 652, 657, 662, 667/4730, 4734, 4748, 4753, 4758, 4763
Group Deleted
639, 641, 649, 654, 659, 664/4735, 4737, 4745, 4750, 4755, 4760
Group Changed
644/4740 – User Acct. Locked Out (Due to Failed Login Attempts)
647/4743 – Computer Deleted
668/4764 – Group Type Changed
671/4767 – User Acct. Unlocked
675/4771 – Auth. Fail-Workstation

4 Challenges of Auditing Active Directory Users and Groups



This PowerShell script makes fast work of a tricky task

by Bill Stewart

I've lost track of how many times someone has asked in an online forum: "How do I list all users and their group memberships in an AD domain?" Third-party auditors or security consultants also ask this question when trying to assess an organization's Active Directory (AD) environment. I decided to write a Windows PowerShell script to address this task. I initially thought that writing such a script would be simple, but four challenges caused the task to take longer than I expected. I'll describe these issues, but first I need to explain the basics of using Microsoft .NET in PowerShell to search AD.

Using .NET to Search AD

When using .NET to search AD, you can use the [ADSISearcher] type accelerator in PowerShell to search for objects. For example, enter the following commands at a PowerShell prompt to output a list of all users in the current domain:

```
PS C:\> $searcher = [ADSISearcher] "(&(objectCategory=user)(objectClass=user))"
PS C:\> $searcher.FindAll()
```

[ADSISearcher] is a type accelerator for the .NET System .DirectoryServices.DirectorySearcher object. The string following this type accelerator sets the object's SearchFilter property to find all user objects, and the FindAll method starts the search. The output is a list of System.DirectoryServices.SearchResult objects.

Next, we want to determine a user's group memberships. We can use the Properties collection from a SearchResult object and retrieve the object's memberof attribute. Using the $searcher variable from the previous example, we can use the FindOne method to retrieve one result and output the user's group memberships:

```
PS C:\> $result = $searcher.FindOne()
PS C:\> $result.Properties["memberof"] | sort-object
```

The first command finds the first user that matches the search filter, and the second command outputs a list of the groups of which that user is a member.

However, if you look carefully at this list, you'll notice that something is missing: The user's primary group isn't included in the memberof attribute. I wanted the complete list of

groups (including the primary group)—which leads us to the first challenge.

Challenge #1: Finding a User's Primary Group

The Microsoft article "How to Use Native ADSI Components to Find the Primary Group" (support.microsoft.com/kb/321360) describes a workaround for the exclusion of the primary group from the memberof attribute. The workaround uses these steps:

1. Connect to the user object by using the WinNT provider (instead of the LDAP provider).
2. Retrieve the user's primaryGroupID attribute.
3. Retrieve the names of the user's groups by using the WinNT provider, which includes the primary group.
4. Search AD for these groups by using their sAMAccountName attributes.
5. Find the group in which the primary GroupToken attribute matches the user's primaryGroupID.

The problem with this workaround is that it requires the script to use the WinNT provider to connect to the user object. That is, I needed the script to translate a user's distinguished name (DN; e.g., CN=Ken Myer,OU=Marketing,DC=fabrikam,DC=com) into a format that the WinNT provider could use (e.g., WinNT://FABRIKAM/kenmyer,User).

Challenge #2: Translating Between Naming Formats

The NameTranslate object is a COM (ActiveX) object that implements the IADsNameTranslate interface, which translates the names of AD objects into alternate formats. You can use the NameTranslate object by creating the object and then calling its Init method to initialize it. For example, Listing 1 shows VBScript code that creates and initializes the NameTranslate object.

However, the NameTranslate object doesn't work as expected in PowerShell, as Figure 1 shows. The problem is that the NameTranslate object doesn't have a type library, which .NET (and thus PowerShell) uses to provide easier access to COM objects. Fortunately, there's a workaround for this problem as well: The .NET InvokeMember method allows PowerShell to get or set a property or execute a method from a COM object that's missing a type library. Listing 2 shows the PowerShell equivalent of the VBScript code in Listing 1.

I wanted the script to handle one other name-related problem. The memberof attribute for an AD user contains a list of DNs of which a user is a member, but I wanted the samaccountname attribute for each group instead. (This is called the Pre-Windows 2000 name in the Active Directory Users and Computers GUI.) The script uses the NameTranslate object to handle this issue also.

Challenge #3: Dealing with Special Characters

Microsoft documentation regarding DNs mentions that certain characters must be "escaped" (i.e., prefixed with \) to be interpreted properly (see msdn.microsoft.com/en-us/library/aa366101.aspx). Fortunately, the Pathname COM object provides this capability. The script uses the Pathname object to escape DNs that contain special characters. The Pathname object also requires the .NET InvokeMember method because, like the NameTranslate object, this object lacks a type library.

Challenge #4: Improving Performance

If you look back at Challenge #1 (Finding a User's Primary Group), you'll notice that the workaround solution requires an AD search for a user's groups. If you repeat this search for many user accounts, the repeated searching adds up to a lot of overhead. Retrieving the samaccountname attribute for each group in the memberof attribute that I mentioned in Problem #2 (Translating Between Naming Formats) also adds overhead. To meet this challenge, the script uses two global hash tables that cache results for improved performance.

Get-UsersAndGroups.ps1

Get-UsersAndGroups.ps1 is the completed PowerShell script, which generates a list of users and the users' group memberships. The script's command-line syntax is as follows:

```
Get-UsersAndGroups [[-SearchLocation]
  <String[]>] [-SearchScope <String>]
```

The -SearchLocation parameter is one or more DNs to search for user accounts. Because a DN contains commas (,), enclose each DN in single quotes (') or double quotes (") to prevent PowerShell from interpreting it as an array. The -SearchLocation parameter name is optional. The script also accepts pipeline input; each value from the pipeline must be a DN to search.

The -SearchScope value specifies the possible scope for the AD search. This value must be one of three choices: Base (limit the search to the base object, not used), OneLevel (search the immediate child objects of the base object), or Subtree (search the entire

Listing 1: Creating and Initializing the NameTranslate Object in VBScript

```
Const ADS_NAME_INITTYPE_GC = 3
Dim NameTranslate
Set NameTranslate = CreateObject("NameTranslate")
NameTranslate.Init ADS_NAME_INITTYPE_GC, vbNull
```

Listing 2: Creating and Initializing the NameTranslate Object in PowerShell

```
$ADS_NAME_INITTYPE_GC = 3
$NameTranslate = new-object -comobject NameTranslate
[Void] $NameTranslate.GetType().InvokeMember("Init", "InvokeMethod",
  $NULL, $NameTranslate, ($ADS_NAME_INITTYPE_GC, $NULL))
```

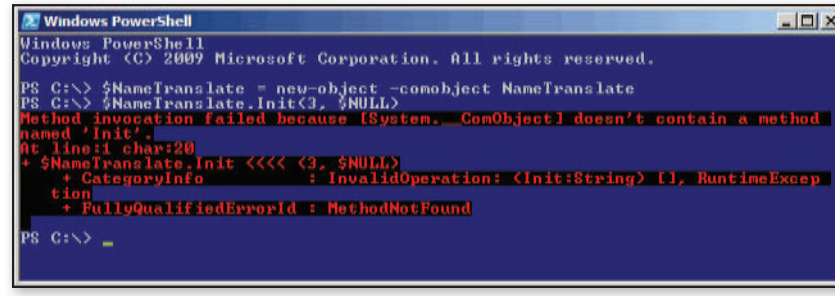


Figure 1: Unexpected behavior of the NameTranslate object in PowerShell

Table 1: The Script's Object Properties

Property	Description
DN	The user's distinguished name (e.g., CN=Ken Myer,OU=Marketing, DC=fabrikam,DC=com)
CN	The user's common name (e.g., Ken Myer)
UserName	The user's logon name (e.g., kenmyer)
Disabled	True if the user account is disabled; False otherwise
Group	The group or groups of which the user is a member

subtree). If no value is specified, the Subtree value is used by default. Use -SearchScope OneLevel if you want to search a particular organizational unit (OU) but none of the OUs under it. The script outputs objects that contain the properties listed in Table 1.

Overcoming the 4 Challenges

The script implements the solutions to the four challenges that I mentioned earlier:

- Challenge #1 (Finding a User's Primary Group): The get-primarygroupname function returns the primary group name for a user.
- Challenge #2 (Translating Between Naming Formats): The script uses the NameTranslate COM object to translate between naming formats.
- Challenge #3 (Dealing with Special Characters): The script uses the get-escaped function, which uses the Pathname object to return DNs with the proper escape characters inserted.
- Challenge #4 (Improving Performance): The script uses the $PrimaryGroups and $Groups hash tables. The $PrimaryGroups hash table's keys are primary group IDs, and its values are the primary groups' samaccountname attributes. The $Groups hash table's keys are the groups' DNs, and its values are the groups' samaccountname attributes.

User and Group Auditing Made Easy

Writing the Get-UsersAndGroups.ps1 script wasn't as straightforward as I thought it would be, but using the script couldn't be easier. The simplest application of the script is a command such as the following:

```
PS C:\> Get-UsersAndGroups | Export-
  CSV Report.csv -NoTypeInformation
```

This command creates a comma-separated value (CSV) file that contains a complete list of users and groups for the current domain. This script lets you effortlessly create the users-and-groups report that your organization needs, in record time.

InstantDoc ID 141463

Bill Stewart
(bstewart@iname.com) is a scripting guru who works in the IT infrastructure group at Emcore in Albuquerque, New Mexico. He has written numerous articles about Windows scripting, is a moderator for Microsoft's Scripting Guys forum, and offers free tools on his website at westmesatech.com.

WINDOWS IT PRO VIP is

Educational—with FREE eLearning courses and eBooks available 24×7

Deep—housing over 41,000 articles on DVD and online, some exclusively for VIP members

Broad—solutions, tips, and tricks for any Windows or SQL Server issue that can stump you

In fact, Windows IT Pro VIP delivers more than **$1,000 of resources and expertise for just $199 a year.**

HOW WINDOWS IT PRO VIP BEATS A SEARCH ENGINE		
	Windows IT Pro VIP Delivers:	**Search Engines Deliver:**
Reliability	Road-tested advice from experts who put their reputation on the line	Well-meaning but potentially harmful tips in the latest Wikipedia entry
Speed	The answers you need in seconds searching by keyword, topic, or publication	Lost time spent perusing sites that have mastered search engine rankings but not the art of Active Directory or patch management
Impartiality	Authors and experts who challenge the Microsoft party line and influence industry change	Conventional wisdom touted by industry insiders afraid to tell it like it is

Order Online Now at windowsitpro.com/go/vip

Windows Server 8 Hyper-V

New high-availability and migration features bring the "wow"

by John Savill

Wow! If I had to pick one word to describe my reaction to the new and improved Microsoft Hyper-V features in Windows Server 8, then *wow* would be it. A little smile crept onto my face when I saw all the features that will put Hyper-V on equal footing—or ahead of—the competition, from a pure machine virtualization–platform feature comparison.

Microsoft has been clear in its message that Windows Server 8 is *the* OS and virtualization platform, for both private environments and the public cloud. Hyper-V provides functionality that allows Windows Server 8 to be a true cloud solution. This typically means enough scalability, flexibility, and security or isolation capabilities to handle all the possible scenarios in a cloud solution that's shared by different business units or even different organizations.

A Bit of Background

Hyper-V was added soon after the release of Windows Server 2008. The original solution offered solid performance, but mobility was limited to quick migration, which required saving virtual machine (VM) memory and state to disk. Because there was no true shared storage, the disk was dismounted from the current host and mounted on the new host; memory and state were then loaded from disk, and the new VM was started. Clients were disconnected during this quick migration—not a popular action. Server 2008 Hyper-V offered no support for NIC teaming.

Server 2008 R2 added live migration, giving a zero-downtime planned-migration capability and allowing all nodes in a cluster to concurrently read and write to a shared NTFS volume (using the Cluster Shared Volumes feature). Server 2008 R2 Hyper-V supports NIC teaming, although implementations vary by vendor. Support for more-advanced networking features, such as jumbo frames and virtual machine queue (VMQ), was also added. Server 2008 R2 Service Pack 1 (SP1) added Dynamic Memory for powerful memory-optimization capabilities and Microsoft RemoteFX for server-side graphics rendering in Microsoft Virtual Desktop Infrastructure (VDI) implementations. However, VMs were still limited to four virtual CPUs (vCPUs), 64GB of memory, and 16 nodes per cluster.

For most organizations, Server 2008 R2 SP1 and Microsoft System Center Virtual Machine Manager (SCVMM) meet the requirements for machine virtualization and provide a great experience. But some companies still want to see improvements in certain areas. As I speak to clients, these wished-for capabilities are the ones I hear about the most:

- scalability of VMs (or more than four vCPUs in a VM)
- ability to migrate VM storage without downtime
- ability to merge snapshots while the VM is online
- more nodes in a cluster

- ability to use live migration to migrate more than one VM at a time and to migrate between unclustered nodes
- fully supported, native NIC teaming solution that can include NICs from different vendors
- network virtualization and isolation
- native Hyper-V cluster-patching solution
- ability to use non-local and SAN options, such as file shares, for VM storage
- larger Microsoft Virtual Hard Disk (VHD) support
- storage deduplication and VHDs larger than 2TB

Windows Server 8 Hyper-V promises to deliver all this and a lot more, with features such as 32 vCPUs per VM, 512GB of memory per VM, 63 nodes in a cluster, 16TB VHDX format, and a native NIC teaming solution that can be managed through the new Metro-style Server Manager and Windows PowerShell. In future articles, I'll dive into these improvements. For this article, I want to look into the high-availability and migration improvements in Hyper-V. Quite frankly, they're awesome.

Server Message Block Share Support

Before Windows Server 8, a zero-downtime migration solution required storage between the two nodes in the VM migration. Both nodes needed to see the storage so that they could access the VM configuration and storage. The only type of storage that multiple nodes could see was external, such as a SAN to which all the nodes in a cluster connected (through a medium such as iSCSI or Fibre Channel) and that was made concurrently accessible through Cluster Shared Volumes.

This external storage requirement can be a major issue for organizations that don't want to invest in that type of infrastructure or that prefer to use a NAS solution. For such organizations, Windows 8 introduces Server Message Block (SMB) 2.2, which features key new capabilities that allow VMs to be stored on an SMB file share, with confidence in the integrity of and connectivity to VM assets.

To use a file share, the file server and Hyper-V servers need to run Windows Server 8. VMs can then be stored on a file share for standalone Hyper-V servers and Hyper-V servers that are part of a highly available failover cluster, as Figure 1 shows. The use of an SMB file share for VMs can be compared to other virtualization solutions that use NFS for file-level remote storage. For great flexibility, multiple file shares can be used within a host or failover cluster.

Other enhancements to SMB in Windows Server 8, such as continuously available file shares, a Microsoft Volume Shadow Copy Service (VSS) provider for remote file shares, and multichannel connectivity for great bandwidth and failover, make the use of SMB for VM storage a first-class solution.

Live Migration

The introduction of live migration in Server 2008 R2 Hyper-V—to enable the movement of VMs between hosts in a failover cluster, with zero downtime and no dropped connections from clients—was a huge benefit. Live migration enabled many scenarios, such as evacuating all VMs from a host to other nodes in a cluster for patching, rebooting, and hardware maintenance, with no loss of service.

Live migration also enabled Performance and Resource Optimization (PRO) and Dynamic Optimization in SCVMM. PRO and Dynamic Optimization perform automatic rebalancing and movement of VMs, based on resource utilization, to ensure optimal performance for the VMs by redistributing them across hosts as resource demands change. The SCVMM Power Optimization feature can also use live migration to consolidate VMs onto fewer hosts during quiet times and temporarily power down unneeded hosts to save power (and then wake them when needed again).

Windows Server 8 builds on the success of Live Migration, broadening its use and scalability for the new scenarios and infrastructure changes that we see in the most recent data centers. Specifically, it adds the ability to perform concurrent live migrations, SMB live migration, live storage migration, and migrations where VMs have nothing in common but a shared Ethernet connection.

Concurrent live migrations. Live migration in Server 2008 R2 was restricted to one concurrent live migration operation between the two nodes in the cluster that was involved in the migration: the current VM owner and the target owner. The reason for this enforcement was fairly simple. Most data centers leverage a 1Gbps network infrastructure. A live migration action is highly network-intensive; all the memory is copied over the network between the hosts, and because the VM is running during the memory copy, several copy passes are required to recopy over memory that changed during the previous memory-copy action. (These copy actions get faster with each pass because the amount of data will be much less with each pass.)

Hyper-V was efficient in its use of the network and would saturate a 1Gbps link. If you performed multiple, simultaneous live migrations between two hosts, the network speed would be split between multiple moves. With the bandwidth split, the copy would take longer for each VM, and more memory would change during

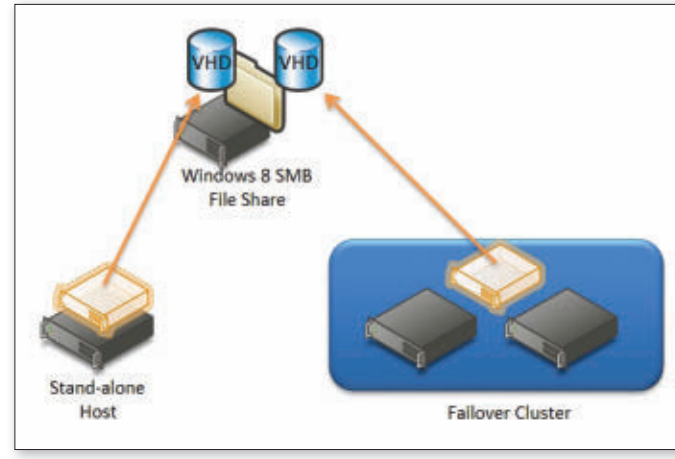


Figure 1: Using a Windows 8 SMB 2.2 file share

Learning Path

To learn more about Windows Server 8:

"Windows Server 8: The Mile-High View," InstantDoc ID 140666

"Exploring Windows Server 8: Dynamic Access Control," InstantDoc ID 140572

"What's New in Windows Server 8 Active Directory," InstantDoc ID 140571

"Windows Server 8 Storage Feature Overview," InstantDoc ID 140577

"Windows Server 8: Hyper-V 3.0 Evens the Odds with vSphere," InstantDoc ID 140573

"Server Management in Windows Server 8," InstantDoc ID 140938

"Top 10: New Features in Windows Server 8," InstantDoc ID 140936

"Upgrading Active Directory to Windows Server 8 (Screenshot Gallery)," InstantDoc ID 141178

the copy, increasing the total time to move the VM.

Think of pouring a bottle of soda through a funnel. Pouring four bottles down the same funnel will take four times as long because the funnel is a limiting factor. Now imagine that as you're pouring out one of those bottles, someone is dripping more soda back into it until it's empty. As a result, the longer you take to empty the bottle, the more soda you actually need to pour, increasing the total pouring time. In this scenario, pouring one bottle's worth at a time actually results in a faster total emptying time for the four bottles.

The funnel is the network, the bottle of soda is a live migration, and the extra soda that's being dripped in is the memory change during the live migration. SCVMM helped handle multiple live migration actions by queuing them and performing them in a series, allowing administrators to queue bulk live migrations in the management interface, and then walk away.

Fast forward: 10Gbps networks in the data center are more prevalent and a single live migration is unlikely to saturate a 10Gbps network link (think "really big funnel"). To accommodate these changes, Windows Server 8 allows multiple concurrent live migrations between hosts. There is no fixed maximum number of concurrent live migrations, although you can specify a maximum number as part of the Hyper-V host configuration. Hyper-V will examine the network capability and the amount of available bandwidth and will tune the number of concurrent live migrations, based on current conditions, to ensure the best performance.

SMB live migration. The enhancements to live migration in a highly available environment are great. But one of the biggest changes is the ability to perform a live migration of a VM outside of a cluster configuration. This capability lets you migrate a VM between two Hyper-V hosts that aren't part of a failover cluster. The two types of live migration outside of a cluster environment are SMB live migration and a shared-nothing live migration.

In an SMB live migration, two Hyper-V hosts both connect to the same SMB file share, which contains the VHDs and configuration files of the VM that is being migrated. The only requirement for the SMB file share is that both Hyper-V host computer accounts must have Full Control rights on the folder and share. The basic mechanics for the live migration are the same as for a live migration within a failover cluster. However, because the VM isn't a shared resource, there are some extra steps:

1. A TCP connection is created between the host that is running the VM (the source host) and the destination host. The VM configuration data is sent to the destination, which allows a skeleton VM to be created on the destination host and a reservation for the required memory to be made.
2. The memory of the VM is copied from the source to the destination. Like a typical live migration, this process consists of an initial complete memory transfer, followed by several iterations to copy over changed memory pages.
3. When the amount of memory that is left to transfer can be copied without significantly affecting the freeze time of the VM, the VM temporarily is stunned. The remaining memory, plus the CPU and device state, are copied to the destination host.
4. The handles to the files on the SMB file share are transferred from the source host to the destination host, along with any physical storage that might be attached through the new virtual Fibre Channel adapter (another great feature in Windows Server 8 Hyper-V).
5. The destination VM is unstunned. The source VM is deleted.
6. A reverse Address Resolution Protocol (ARP) packet is sent out, forcing network switches to update their mapping of the VM IP address to the MAC of the new host.

The VM is typically unresponsive for just milliseconds—way below TCP connection timeouts, so there's no effect on VM users. If you sat and watched a ping to the VM that was being migrated, you might see a longer than usual response time for one ping packet (or even a dropped packet), but nothing that a user would notice or that would cause a disconnection.

Live storage migration. Before I talk about the shared-nothing live migration capability, I want to introduce another type of live migration. Live storage migration allows a VM's storage (such as its VHDs) and configuration files to be moved while the VM is running. Moving VM storage can be useful in a variety of scenarios:

- moving a VM from local storage to a SAN
- moving VMs between SANs for rebalancing I/O or performing maintenance on a SAN
- moving VMs to an SMB share
- emptying an NTFS volume of VMs so that you can run a chkdsk operation

Whatever the reason, Live Storage Move allows you to move VM files between all supported storage mediums—DAS, SAN, and file-based (e.g., SMB)—with no downtime for the VM.

Live storage migration works differently from live migration. Live migration works with memory, which can be read to and written to quickly. Therefore, performing iterations of changes since the last copy works. But for storage, those many iterations might never catch up for busy disks.

As Figure 2 shows, the live storage migration process involves several steps

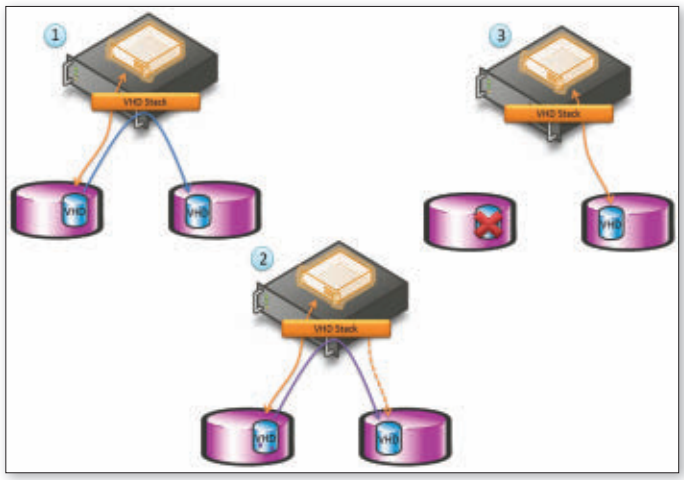


Figure 2: Three main stages of a live storage migration operation

that solve the problem of the comparative slowness of physical disks. In step 1, an initial copy is made of the storage, which includes the VHD files, configuration files, snapshots, and everything related to the VM. During this time, the VM reads and writes to the source storage. In step 2, after the initial copy is complete, the VHD stack mirrors all writes to both the source and destination storage locations, while making a single pass of copying the blocks that changed during the initial copy. Finally, in step 3, both the source and target are synchronized. The VHD stack switches the VM to read and write to the target storage only and then deletes the data on the source storage. The result is a complete move of the storage that's associated with the VM, with no downtime.

Shared-nothing live migration. If I had to pick one feature that's behind my "wow" reaction, this would be it: the ability to migrate a VM from one Hyper-V server to another Hyper-V server that isn't part of the same cluster, shares no storage, and has only a Gigabit Ethernet connection to the first VM—all with zero downtime!

Shared-nothing live migration looks very like SMB live migration. But this time, we also need to move the storage, using the technology I just discussed for live storage migration. We're essentially performing everything in the SMB live migration scenario, *plus* a live storage migration, *and* maintaining the mirroring of writes to both the source and destination storage while performing a live migration of the memory and state, before finally switching the host that's running the VM.

With shared-nothing live migration, we can move VMs between any Windows Server 8 Hyper-V hosts, even when they have nothing in common but a shared Ethernet cable. I've seen a great demonstration of the shared-nothing live migration between two laptops, each with only local storage. The running VM that uses local storage moves to the second laptop, without any downtime for the VM. Now, imagine the same capability being used to move VMs between clusters, hosts, or even private and public cloud Infrastructure as a Service (IaaS) providers.

During a disaster, an administrator must manually activate Hyper-V Replica.

Hyper-V Replica

All the live migration technologies, including live storage migration, are used in planned migrations in typical day-to-day scenarios. Organizations face a completely different set of challenges when thinking of disaster recovery, which requires a different set of solutions.

Numerous solutions provide disaster-recovery capabilities for Hyper-V environments. However, these solutions typically involve expensive storage solutions that might be unavailable to small and midsized organizations. Hyper-V Replica, another new feature in Windows Server 8, allows asynchronous replication of a VM's storage from one Hyper-V host to another, even if the hosts are using completely different types of storage. An initial replication of the source VM's storage is performed over the network (by using a direct connection between the primary and replica server) or by saving the VM's storage to a network location from which the replica server reads. This approach is known as off-the-network seeding.

If there is insufficient bandwidth for the initial storage seeding on the replica to occur over the network—for example, when creating a replica at a remote location from a VM with large amounts of storage—then a backup can be taken of the VM on the primary server. This backup is shipped to the replica server and restored.

When the initial replication of the VM is completed, a delta replication of the VM storage is performed every 5 minutes. Because this replication is asynchronous and periodic, it isn't a real-time replication solution. In the event of an unplanned outage, a few minutes' worth of storage data could be lost when failing over to the replica—a factor that should be considered when architecting a solution that uses Hyper-V Replica. However, the benefit of this asynchronous replication is that there are no limitations on the scale of the VM to be replicated or high requirements for the network between the primary Hyper-V server and the replica. The exact bandwidth that's needed between the servers depends on the amount of storage change. However, some of the planned scenarios of Hyper-V Replica include a replica in a secondary site, connected via a WAN link.

Hyper-V Replica is not an automated failover solution. During a disaster, an administrator must manually activate the feature. Options exist to test the failover process and run the replica VM that connects to a separate test network so that it doesn't interfere with the production primary VM. In planned scenarios, the primary VM is shut down manually, and a final delta is sent to the replica, which applies the delta and then starts a reverse replication to what was the primary VM.

The actual configuration of Hyper-V Replica is a fairly simple process. Replication configuration is now a setting

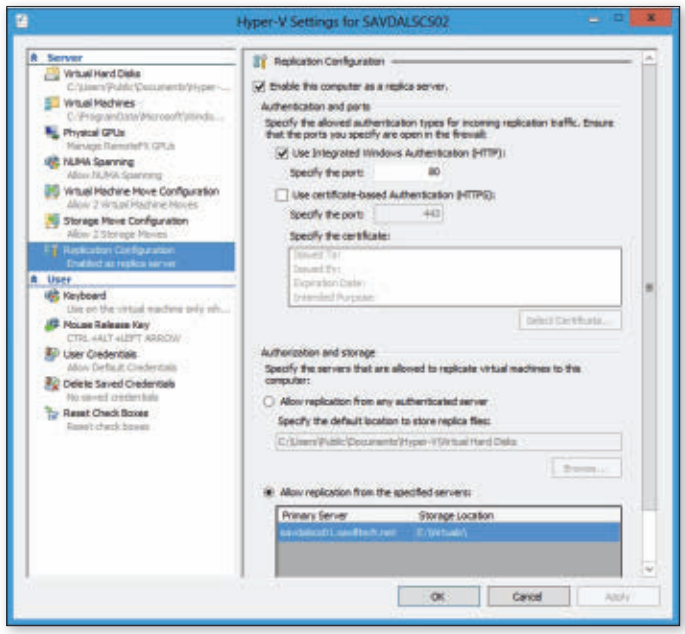


Figure 3: Enabling a server to be a replication target

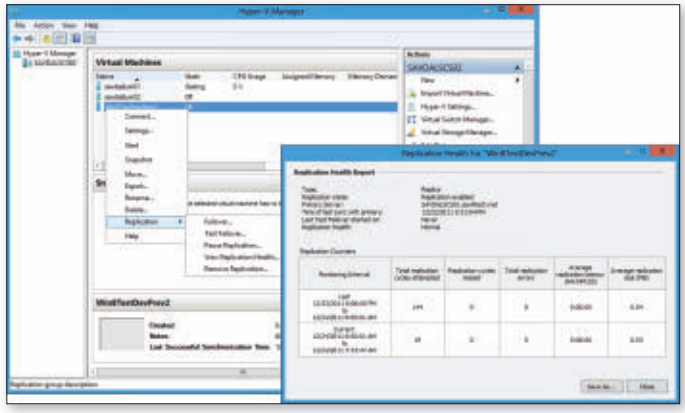


Figure 4: Insight into the state of the replica and easy control of failover and management

on all Hyper-V servers. That setting can be enabled with the option to use integrated Windows Authentication, with replication of the changes over port 80 (HTTP), or certificate-based authentication, with replication over port 443 (HTTPS). The latter type of authentication also provides encryption of the VM update data when it's sent over the network. The ports that are used can be changed for the replication configuration. Also, a server can be configured to accept replication from any Hyper-V server or specific Hyper-V servers, as Figure 3 shows. The only additional step on the replication target is to enable firewall rules to allow communication over the selected ports.

When a Hyper-V server that has replication enabled is available, a VM can be configured to have a replica through an Enable Replication action. When replication is enabled, the administrator is prompted to specify the target replica server and how the initial replication should be performed. The replication also allows you to create a certain number of optional recovery points, which are hourly VSS snapshots that ensure the integrity of the specific replica recovery point. The VM replicates, and the replication health can be checked at any time through a health report option that shows the number of replication cycles, the average size of the replication, and the time that the replication has been happening, as Figure 4 shows. You can also configure an alternate TCP/IP configuration for the replica VM when it's activated. This alternate configuration must be injected into the VM if the replica is hosted in a different network and network virtualization isn't used (another great feature of Windows Server 8).

Understanding Hyper-V Replica is important. The feature is intended for small or midsized businesses that want secondary-site disaster-recovery capability. Hyper-V Replica works by periodically sending VM storage updates to the second location. During a disaster, the replica is activated and the OS starts in a crash-consistent state at the point of the last storage delta from the primary. If this crash-consistent state isn't good enough, and if the recovery point feature is enabled, the administrator can select a recovery point. This point starts the replica at a VSS snapshot point, which ensures that the VM is in an application-consistent state. This out-of-the-box feature gives a good level of disaster-recovery protection without requiring high network speeds, and supports any type storage that Hyper-V supports. However, the feature isn't real-time or automated, so if you need a higher level of functionality, you should look at third-party solutions that build on Hyper-V.

Great New Capabilities

The new Windows Server 8 features for VM migration and replication give organizations a great new capability for keeping VMs available and mobile throughout an organization's IT infrastructure—without needing complex and expensive infrastructure changes. The Hyper-V live migration and Replica capabilities are just a few of the enhancements, and this discussion is based on the beta of Windows Server 8 so functionality could change. But the features give us an idea of the level of advancements that we're going to enjoy in the next version of Hyper-V and Windows Server.

InstantDoc ID 141821

John Savill
(john@savilltech.com) is a Windows technical specialist, an 11-time MVP, and an MCITP: Enterprise Administrator for Windows Server 2008. He's a senior contributing editor for *Windows IT Pro*, and is currently writing his fifth book, *Microsoft Virtualization Secrets* (Wiley).

Paul Thurrott...

. . . he's not in Microsoft's pocket, but now he can be in yours.

The independent voice for IT enthusiasts

Paul Thurrott delivers news, tips, commentaries, and reviews on Microsoft technology – from gaming to mobile to servers to software, and coverage of Microsoft competitors in between. Get daily updates without reaching farther than your pocket.

Download your
Paul Thurrott: PocketTech app today

windowsitpro.com/mobile-apps

Available for iPhone | Windows Phone 7 | Android

7 Important Exchange Server Innovations

Technical advances make the cloud feasible

by Tony Redmond

The benefit of hindsight is a wonderful gift to technologists. It lets us understand how changes that were made in the past laid the foundation for current capabilities. In the case of Microsoft Exchange Server, three types of deployment are now possible: classic on-premises, cloud with Microsoft Office 365, and hybrid, in which some parts of the infrastructure reside on premises and some reside in the cloud.

Exchange didn't arrive at this point by accident. The Exchange development group has done a lot of heavy lifting over the past decade so that customers can enjoy the choices they have today. Looking back, I see seven important areas in which innovation has liberated Exchange from its origins as a LAN-based email server running on Windows NT. Apart from all else, I think that these areas represent the most crucial areas for Exchange administrators to master in the foreseeable future.

The Magnificent Seven

Perhaps it's unfair to focus on just seven areas, when Exchange is now a huge product that spans well over 20 million lines of code. I freely admit that other areas of innovation within Exchange deserve consideration.

For example, there's the elegance of single page patching within a database availability group (DAG). This implementation allows the Information Store to detect page corruptions and then broadcast requests to other database copies to retrieve the data necessary to fix the problem, all while keeping the database online and serving users.

Even so, I'm happy to stay with the group that I've selected. In no particular order of importance, these are my chosen areas of innovation:

1. Remote Procedure Call (RPC) over HTTP
2. Windows PowerShell
3. Autodiscover service
4. Mailbox Replication Service (MRS)
5. Multibrowser interfaces
6. Storage improvements
7. Client Access server

Now, let me explain my logic.

#1: RPC over HTTP: Eliminating VPNs

In the early days of Exchange, remote access was characterized by synchronization woes, slow dial-up connections, and VPNs. Improvements in client technology—such as the drizzle-mode synchronization that Microsoft Office Outlook 2003 introduced—and the now-ubiquitous nature of fast wireless

connections have eliminated the first two issues. And the need to establish a VPN before connecting to Exchange was firmly whacked on the head by the introduction of RPC over HTTP in Exchange Server 2003.

Now known as Outlook Anywhere, RPC over HTTP was initially difficult to configure. Those who persisted and published the necessary public connectivity points discovered that Outlook could connect easily. Furthermore, it could use the public Internet to transport, safely encapsulated in HTTP packets, the Messaging API (MAPI) remote procedure calls (RPCs) that form the basis of any communication between Outlook and Exchange. Administrators loved the fact that ports 80 and 443 were the only ones that they needed to open in the firewall, especially because these ports are usually open to support other web-based applications.

Since Exchange 2003, Microsoft has gradually improved the configuration and management of this component. Now, Outlook Anywhere is a real strength of the product, so much so that it provides the fundamental underpinning of both Microsoft Business Productivity Online Standard Suite (BPOS) and Office 365.

After all, requiring every customer to create a VPN to access Microsoft Exchange Online would be impossible and too expensive to create and maintain for many small-to-midsized businesses (SMBs). Such a requirement would also create a huge burden for Microsoft, which would need to manage the incoming VPN connections.

Simply put, Outlook Anywhere allows everyone to connect across the Internet. Plus, the $6 per month price point for Office 365 is feasible. That's why RPC over HTTP is #1 on my list.

#2: PowerShell: Delivering a Common Management Platform

PowerShell might seem a strange choice for #2. But its introduction in Exchange Server 2007 and subsequent upgrade to remote PowerShell in Exchange Server 2010 have delivered many benefits. First, PowerShell provides consistency across the management interfaces within Exchange. In other words, you can use the Exchange Control Panel (ECP) to update a mailbox's properties in Office 365, or you can run the Set-Mailbox cmdlet by using PowerShell. Both routes lead to the execution of the same logic.

But my main reason for selecting this component is that the advent of remote PowerShell delivers the ability to manage Exchange Online without needing to log on to the servers on which Exchange runs. Obviously, Microsoft couldn't permit thousands of Office 365 customers access to mailbox or Hub Transport servers. But remote PowerShell allows domain administrators to connect across the Internet and validate their credentials for a tailored session that contains the exact set of cmdlets that they're allowed to run. And because PowerShell forces all paths to the same logic, the user can connect by running Exchange Management Shell (EMS), or through ECP, or through the Microsoft Management Console (MMC)-based Exchange Management Console (EMC): Everything works in the same way. That's why PowerShell is my #2 choice.

PowerShell provides consistency across the management interfaces within Exchange Server.

#3: Audodiscover: Solving User Pain

Microsoft introduced the Autodiscover service in Exchange 2007 as a solution for the perennial problem in which users had trouble configuring Outlook with the parameters that were necessary to connect to Exchange. The basic difficulty: Server names that make perfect sense to administrators put users into a deep sleep. Apparently, regular users have problems coping with names such as EXSERVER1 or MBXHUB-LONDON.

Microsoft figured out that the issue could be solved by making computers communicate to figure out a user's mailbox location. That's what Autodiscover does, by consulting signposts such as a service connection point (SCP) in Active Directory (AD) to retrieve information about Exchange and to discover a mailbox's current location. Of course, AD is available only inside a firewall, but Autodiscover can use URLs that are published to the public Internet to retrieve what it needs. This capability laid the foundation to allow easy connection to Exchange Online in BPOS and Office 365. Without Autodiscover, administrators would face far more complexity and cost when they configured user PCs to connect to the cloud.

Autodiscover works well for Outlook 2010 and Outlook 2007, the only two clients that support the feature. Microsoft expanded the information that Autodiscover returns to the client. Autodiscover can now retrieve data about alternative mailboxes that Outlook should open (i.e., mailboxes to which the user has been granted full access) and URLs that map Exchange services such as the Offline Address Book (OAB) distribution point, Exchange Web Services, Unified Messaging, and so on. Exchange returns all this information as XML data to Outlook, which refreshes the information every 15 minutes to ensure that it keeps up-to-date with any changes.

You can use Outlook's Test E-mail AutoConfiguration option to gain an insight into the information that Autodiscover retrieves. To run the option, press CTRL and right-click the Outlook icon in the system tray and select Test E-mail AutoConfiguration from the menu. Clear the Use Guessmart and Secure Guessmart Authentication options, enter your email address and your password, and click Test. Outlook goes through the same process that it uses when it populates a user profile for the first time. Click the XML tab to see the data returned by Exchange.

As Figure 1 shows, this data includes details such as the server name and the URLs that are necessary to connect to Exchange Web Services (EwsUrl) and ECP (EcpUrl). In this example, I've connected to my Office 365 mailbox, so the results are those that come back from Office 365.

It's worth noting that Autodiscover is one reason why Microsoft doesn't support connecting Outlook 2003 clients to Office 365. Although you could manually configure all the server settings in Outlook 2003 to make a connection to a cloud-based mailbox, the automatic nature of profile updates that Autodiscover performs in Outlook 2010 and Outlook 2007 facilitates easy movement of mailboxes between servers. Microsoft continually adds servers

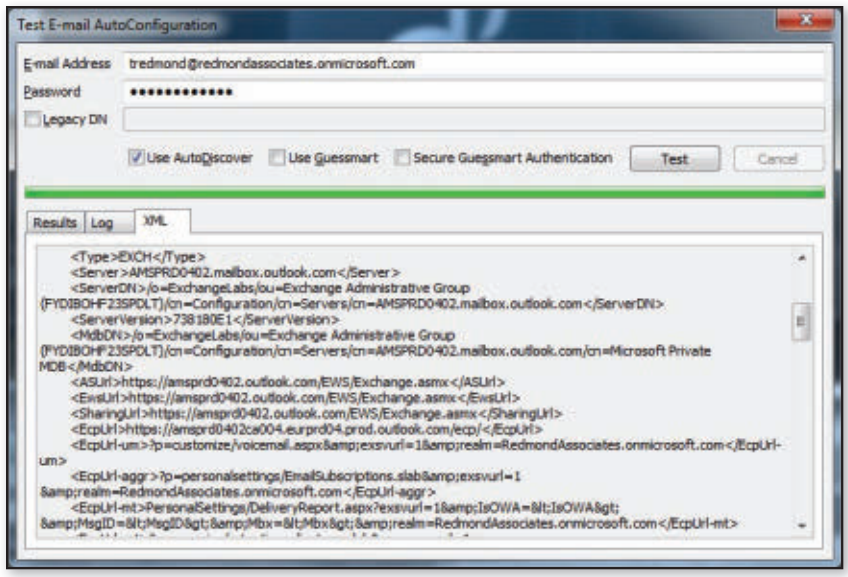


Figure 1: Results of an Autodiscover test run

as it builds out its Office 365 infrastructure, and then rebalances workload across available servers by transferring mailboxes between databases. If Outlook 2003 clients were connected, users would need to know what to do if their mailboxes were moved. The result might be a support nightmare. Restricting support to Outlook 2010 and Outlook 2007 solves that potential support headache and encourages users to upgrade to software that can take advantage of the most recent server features (e.g., MailTips), so it's a logical win-win situation for Microsoft.

Autodiscover keeps Office 365 administrators from running around to help users more than they already need to do, so it's a good choice for #3.

#4: Mailbox Replication Service: Smooth, Elegant Moves

Large mailboxes are all the rage today. I can't quite understand why, as the vast majority of humans take a long time to fill a 25GB mailbox. Still, the advent of massive mailboxes has made the task of moving them a much more complex business than it used to be.

Until Exchange 2010, administrators had to ask users to log off before their mailboxes could be moved. The mailboxes moved in real time, and nothing could be done until the full and complete mailbox reached its destination. If something happened during the move, you had to restart. Although workable, this solution is ineffective when mailboxes need to move from on-premises servers to the cloud and vice versa. And as I mentioned earlier, Microsoft needs to operate in a state of almost perpetual mailbox moves to rebalance databases as it builds out its Office 365 infrastructure.

Cue the introduction of MRS in Exchange 2010. Mailbox moves now occur in the background, with frequent checkpoints and sufficient intelligence to acknowledge when the receiving server might be under pressure. Although moves cannot be scheduled (a deficiency that Microsoft will surely address in the future), they can be auto-suspended. Such moves copy an initial snapshot of a mailbox's contents, in the background, and then pause. An administrator can check the mailbox move report and resume the move if all seems well. MRS then takes another snapshot of the source mailbox and performs an incremental synchronization before switching pointers in AD to direct the user to the new location.

Best of all, MRS is extremely competent at transferring mailboxes between AD forests, from on-premises deployments to the cloud, and between versions of Exchange (from Exchange 2003 onward). Without the service it's difficult to see how Microsoft could cope with the transfer of millions of mailboxes to Office 365; the manual workload involved in setting up and managing mailbox moves across the Internet would be massive and costly. Instead, many organizations use the auto-suspend technique to move mailboxes in the background, as many as 30 days before a user is finally transferred to Office 365.

And MRS does more than move mailboxes. Microsoft has expanded its responsibilities to manage tasks such as import and export of mailbox data from personal folder stores (PSTs) and mailbox restore requests. Because of its key role in mailbox management, I think MRS deserves its position as #4 on my list.

#5: Multibrowser Support

No self-respecting cloud service can run without offering browser support. In Exchange, browser connectivity began in 1997, when Exchange 5.0 shipped the first version of Outlook Web Access (OWA), now charmingly renamed Outlook Web App (but still OWA). In truth, the first version of OWA wasn't very good. But much has been learned about browser interfaces, standards, and functions since 1997.

Today's OWA boasts a solid and highly functional UI that puts competitors such as Google Gmail to shame. OWA connects with ease to both on-premises and cloud versions of Exchange and supports a rich user experience on Internet Explorer (IE), Google Chrome, Mozilla Firefox, and Apple Safari. Other browsers can connect with the basic version of OWA—still highly usable, even if missing some of the bells and whistles of its premium counterpart.

An equally important evolution is occurring for browser-based management interfaces. Exchange 2010 introduced ECP—and promptly confused administrators because some tasks, such as discovery searches or ActiveSync device policy maintenance, can be performed only through ECP. No trace of these tasks appears in the flagship EMC. Equally frustrating, some tasks, such as DAG management, show up only in EMC. For example, DAG management can be performed only through EMC, which boasts other convenient features such as wizard-based execution of complex tasks (e.g., certificate management) and the ability to show administrators the underlying PowerShell code that will be executed to accomplish a task.

However, the important thing to realize is that ECP is in its first iteration. Web-based management is a crucial piece of the evolution of Exchange Online within Office 365. Over time, I expect more and

more administrative tasks to show up in ECP, until the need to maintain two management consoles disappears. I predict a time when Microsoft removes EMC from Exchange, leaving us with a single browser-management client that hopefully includes all the EMC features that administrators depend on.

ECP already supports the same range of browsers as OWA, and Exchange 2010 Service Pack 1 (SP1) introduced the ability for users who aren't mail-enabled to use ECP to perform administrative tasks. Because of their key roles for both users and administrators (today and in future cloud services), I give the OWA/ECP combination the #5 slot on my list.

#6: Storage: Cheap and Cheerful Bytes

Storage was the single biggest cost bucket for Exchange 2003 deployments. This can be partially explained by the cost per gigabyte back in 2003 to 2005, but the I/O profile that Exchange generated was more relevant. To be blunt: Exchange 2003 was an I/O hog. The only way to get reasonable performance was to deploy expensive storage that could deliver the required I/O operations per second (IOPS) performance to support the desired number of mailboxes. SAN storage—expensive to buy and equally expensive to set up and maintain for Exchange—was often necessary.

Microsoft tweaked the Information Store in Exchange 2007 to improve its I/O profile, with considerable success. Fundamental change then occurred in Exchange 2010, with the first database schema change since Exchange Server 4.0. Many other updates were made to drive down I/O requirements and deliver the ability to run Exchange on cheap DAS and Just a Bunch of Disks (JBOD) arrays. As a result, the I/O requirement of one IOPS per mailbox that existed in Exchange 2003 is now down to circa 0.1 IOPS. Furthermore, Exchange 2010 can process huge mailboxes stuffed with hundreds of thousands of items—a situation that would have brought Exchange 2003 to its knees.

If Microsoft hadn't invested in the engineering effort to make such a dramatic improvement to database performance, it wouldn't be able to offer 25GB mailboxes in all but the most basic Office 365 kiosk plans, and it would be unable to compete with Gmail. For those reasons, storage improvements are innovation #6.

#7: Client Access Server: Exchange's Black Box

The Client Access server role first appeared in Exchange 2007, as the common endpoint for Internet protocols. The role was then enhanced with the RPC Client Access layer in Exchange 2010, to become the endpoint for MAPI clients. The Exchange 2010 Client Access server also hosts MRS, so it plays an important role in mailbox moves.

The transition from mailbox server to Client Access server is why I think this component is important. Without the Client Access server, Exchange would have been unable to break the connection between mailbox and server that existed prior to Exchange 2010. The high availability gained through DAGs would also have been impossible because we would be unable to switch databases easily and quickly between servers. And without DAGs, Microsoft probably would have been unable to deploy Exchange Online as it has, with multiple database copies split across geographically separate data centers. The upshot is that Microsoft might not be able to offer the financially backed 99.9 percent service level agreement (SLA) that it offers for Office 365.

> Exchanged has evolved over the years and can now handle three very different kinds of deployment.

But there's more. The Client Access server is key to the effective management of incoming client connections. On-premises administrators will be aware of the interaction between firewalls, load balancers, and the Client Access server to manage HTTP, MAPI, IMAP4, POP3, and ActiveSync clients. Between Windows Server 2008 R2 and Exchange 2010, important changes—such as the ability to combine individual Client Access servers into Client Access server arrays and better handling of session identifiers—allow servers to handle a greater volume of connections more effectively. This ability is hugely important, given the tens of millions of clients that Office 365 is expected to manage. That's why the Client Access server takes the final position in my list.

I'd be happier with my choice if Microsoft provided functions to allow administrators to understand exactly what the Client Access server is doing at any point. Right now, the Client Access server is often a black box, with connections going in and out with no indication of whether everything is progressing as expected. Perhaps Microsoft will do something to improve the telemetry and feedback from the Client Access server in a future version of Exchange, if only to help the folks who run Office 365.

What's Next?

I won't be offended if you disagree with the logic behind my choice of the magnificent seven. Have fun reordering my list to assign your best idea of the relative importance of each component. The important thing is that Exchange has been gradually evolving over the years, to the point that it can now cope with the demands of three very different kinds of deployment.

I'm not sure that the engineers realized how all these pieces would fit together when they set out to design any one component, but blessed serendipity has brought us to the current situation. I'm quite sure that development isn't complete and that you'll see massive evolution in Exchange over the next few years, as the product heads for its 20th anniversary in 2016. If we revisit the assessment at that time, I think some of the same components will be on the list. The question is which new components will appear over the next four to five years?

InstantDoc ID 141204

Tony Redmond
(tony.redmond@windowsitpro.com) is a contributing editor for *Windows IT Pro* and the author of *Microsoft Exchange Server 2010 Inside Out* (Microsoft Press). He blogs about Exchange and related topics at www.windowsitpro.com/go/ExchangeUnwashed.

Get the Most from Your Desktops with MDOP

Use the Microsoft Desktop Optimization Pack to maximize your desktop-management experience

by John Savill

Windows 7 brings an amazing set of features to today's desktop and other client form factors. For larger organizations, Windows 7 Enterprise adds features that provide a true enterprise-ready OS with more capabilities than Windows 7 Professional, including DirectAccess, BranchCache, Windows BitLocker Drive Encryption and BitLocker To Go, AppLocker, and Enterprise Search Scopes. For organizations that truly leverage these features, users gain huge benefits in usability and the IT organization gains better manageability and security. These capabilities also can often simplify the environment and save money by removing the need for certain third-party add-ons.

Windows 7 Enterprise provides a fantastic client experience. But to fully optimize the desktop from an IT operations perspective—to deliver the best application delivery, inventory, compatibility, and execution experience plus great troubleshooting and management—Microsoft offers the Microsoft Desktop Optimization Pack. MDOP is available as an annual subscription, priced per PC and available to organizations with Software Assurance or Windows Intune, the new Microsoft Software as a Service (SaaS) cloud-based PC-management solution. If your organization has access to Windows 7 Enterprise, you can subscribe to MDOP, generally at around $10 per desktop per year.

In 2006, Microsoft purchased Softricity and Winternals and combined those companies' products with its Desktop Error Monitoring (DEM) solution to create the first version of MDOP. Additional acquisitions of AssetMetrix, DesktopStandard, and Kidaro plus plenty of in-house work resulted in MDOP 2011 R2. This version includes a host of desktop-optimization tools:

- Application Virtualization (App-V)
- Microsoft Enterprise Desktop Virtualization (MED-V)
- Asset Inventory Services (AIS)
- Advanced Group Policy Management (AGPM)
- Microsoft BitLocker Administration and Monitoring (MBAM)
- Diagnostics and Recovery Toolset (DaRT)

App-V

Many organizations that have heard of MDOP think first of App-V. This application-virtualization solution is commonly thought of as the flagship component of MDOP and is certainly the most used.

App-V lets you execute applications on an OS instance without those applications actually being installed. This execution without installation is achieved by a creating a virtualized version of the application, through a process known as sequencing.

Sequencing involves creating a clean OS environment that runs the App-V Sequencing component. This component takes all the changes to the file system, registry, COM, user mode services, fonts, and so on that are made during an actual installation and places that data into virtual layers, such as a

virtual file system and virtual registry, inside a binary stream. This binary stream, which holds the layers that contain the installed version of the application, can then be streamed to App-V clients, into an instance of the App-V virtual environment.

The application then runs in that virtual environment. The application's interaction with the local OS goes through the virtual layers. The application is unchanged; it thinks that it's reading from the OS storage for its program files, which are actually in the virtual layer. The same process applies to components such as the registry, user services, and fonts.

This approach of running applications without needing to install them brings a number of benefits:

- Application-to-application incompatibilities resulting from any kind of clash (such as DLLs or configuration) are solved. Every virtual application runs in its own virtual environment, which can't see the virtual environments of other applications.
- The time required to get new applications or application updates is significantly reduced. Testing no longer needs to include the many combination-scenario tests to determine whether app A works if apps B and C are installed because the applications don't see one another.
- The OS stays cleaner and doesn't experience bloat over time.
- Applications can be delivered to users almost instantly, on demand. No installation is required, only the content of the stream needs to be transferred to the client, and only the part of the stream that's used to initially launch the application—maybe 20 percent of the total stream size—is necessary; the rest is streamed in the background.

Most applications can be virtualized through App-V. If you need virtualized applications to communicate with each other outside standard OLE methods, App-V now features a capability called Dynamic Suite Composition—a fancy name for the ability to create links between virtual applications so that they can share a virtual environment. The only restriction on App-V is that it can't virtualize drivers, system services, or components of the OS, including Internet Explorer (IE). But we have a different solution for IE.

MED-V

MED-V is the solution for applications that won't run on Windows 7 but that work fine on Windows XP. In App-V, the application still fundamentally runs on the local OS; if the application won't run on Windows 7, then virtualizing the application through App-V does nothing to help. MED-V works by running an XP virtual machine (VM) under the covers, using Windows Virtual PC, into which you install those applications that you can't make run on Windows 7 or for which no Windows 7–compatible version or viable alternative is available.

The user experience is seamless. As with App-V, there's no real indication when running an application that's being served through MED-V that the application isn't a local application. The application shortcuts

> MDOP offers great value for any organization, even if you use only one part of the suite.

are part of the Windows 7 Start menu, the launched application is displayed seamlessly on the Windows 7 desktop, icons appear in the Windows 7 system tray, and access to Windows 7 drivers and printers is available. The only hint the user might get that something is a bit different is that the application will have the XP border, plus the dialog boxes and the feel of the application will be those of XP.

I mentioned that App-V can't virtualize IE, which is considered part of the OS. Many organizations, when moving to Windows 7, still need access to IE 6, either because they have systems that don't work with IE 9 or because upgrading to support IE 9 is cost-prohibitive. MED-V uses XP, which includes IE 6, but it has another great feature. You can define URLs in the MED-V configuration so that users are automatically redirected to an IE 6 instance inside MED-V when they launch IE via the Run command or try to access the URLs in IE 9. Therefore, the end users don't need to do anything different to continue accessing sites that require IE 6.

If you've dismissed earlier versions of MED-V, look again at the version that's provided as part of the current MDOP. The separate MED-V infrastructure that was previously required has been removed, and deployments are now available as installation packages that you simply deploy to clients by using standard software-deployment mechanisms or by making them part of your Windows 7 image.

App-V and MED-V both enable great application-management and application-delivery technologies that can improve the way in which your IT organization provides applications and supplement traditional application-deployment solutions. However, keep in mind that MED-V is the one MDOP component that no one really wants you to run for the long term. When planning your Windows 7 deployment, don't rush the move to Windows 7, planning to run everything in MED-V until you have time to test applications in the new OS. MED-V is for those few showstopper applications that just won't run on Windows 7 and that will halt your migration if you can't find a way to make them available on the Windows 7 desktop. You should still look for alternatives to those applications so that you can retire MED-V at some point.

AIS

MDOP's AIS component provides detailed asset information about your environment, for both hardware and software. This component is provided as a cloud service, requiring no infrastructure in your local environment and making AIS quick to deploy. The only setup requirement is to deploy the AIS client to the machines whose inventory data you want to capture. You can perform this step by using Group Policy or any other software-deployment solution.

AIS works a little differently from traditional inventory solutions, particularly from a software-inventory perspective. Most software-inventory solutions query Windows Management Instrumentation (WMI) and retrieve information based on the Win32_Product class, which is also shown in the Programs and Features

Control Panel applets. AIS uses this information but also looks at artifacts on the OS to help identify software that might not show up in WMI and to get more detailed information. The information that's found is then sent to the Microsoft cloud and compared against a dynamic, constantly updated catalog. This method helps identify the installed software and details about that software.

The actual management of AIS is performed via a web-based console that lets you view detailed inventory information for all machines, plus gives you the ability to run reports about all software and hardware. But AIS also goes a step further by letting you import licensing information, enabling reports that show what you're running and what's licensed so that you can ensure license compliancy for your organization. AIS has a great security policy to ensure that only your organization can see your license and inventory information, and everything is encrypted. It's a great tool for your organization to understand your license position and to track your assets.

If you're using Microsoft System Center Configuration Manager (SCCM), then you already have a similar capability. The SCCM Asset Intelligence feature leverages the same dynamic catalog that AIS uses to identify detailed information about software, so you'll probably need to use AIS only on machines that you don't manage with SCCM.

AGPM

I don't think there's a company out there that doesn't use Group Policy in its environment. Just look at the Group Policy functionality advancements that we've seen in Windows Server 2008 R2 and Windows Server 2008, with new features such as Group Policy Preferences, new XML-based formats, improved Group Policy application based on network circumstances, and the sheer number of available configuration options: If you aren't making heavy use of Group Policy, you definitely should be. One item that hasn't quite kept up with the pace of advancement is the management of Group Policy. Although improving, this capability still lacks some key features. That's where the AGPM component of MDOP swoops in to save the day—or at least the administrator's sanity.

AGPM adds the ability to check out and check in Group Policy Objects (GPOs) from a new Group Policy store, to make changes to GPOs without actually applying the changes, and to manage the change control of GPO application. AGPM also adds the ability to delegate groups of users to perform different levels of GPO modification and deployment, through built-in roles for Editors (who can modify GPOs), Reviewers (who can view and compare GPOs), and Approvers (who can create and deploy GPOs). AGPM can also integrate with email to send notification to approvers when an approval is needed.

AGPM has a small server component, which can be installed on any server or on your domain controllers (DCs). The client-side component integrates easily with the existing Group Policy Management Console (GPMC), to which it adds a Change Control node, which Figure 1 shows. This node lets you configure GPOs as Controlled, giving you the full capabilities of AGPM to manage those GPOs.

MBAM

The newest addition to the MDOP suite is MBAM, which gives us enterprise-class management of the BitLocker feature. This type of management was previously restricted to a limited set of Group Policy controls that let you set the level of encryption and determine whether to require BitLocker To Go for removable media and whether recovery keys should be stored in Active Directory (AD).

MBAM provides both improved management capabilities and better insight into the state of the BitLocker environment. The component does this through built-in reports, which can be extended through standard SQL Server Reporting Services (SSRS) methods.

Administrators can set how BitLocker should be used on desktops in the environment. This policy will then be enforced. For example, you can ensure that volumes are enabled for BitLocker but also add exceptions for hardware that doesn't meet requirements or users that have a valid reason not to use BitLocker. When additional volumes are added or a user disables BitLocker, MBAM walks the user through enabling or re-enabling BitLocker encryption, ensuring the security of your devices.

MBAM radically improves the BitLocker end-user experience. With MBAM, standard users can now manage their BitLocker environment, initiate encryption, and set up BitLocker—tasks that were previously restricted to local administrators. Another great feature comes in handy when things go awry and users need the BitLocker recovery key. When BitLocker is enabled, a recovery key is generated. That key can be typed in manually at the BitLocker recovery screen to enable the OS to boot in times of distress.

Typically, users are prompted to save this key to disk, or print it, or tattoo it on

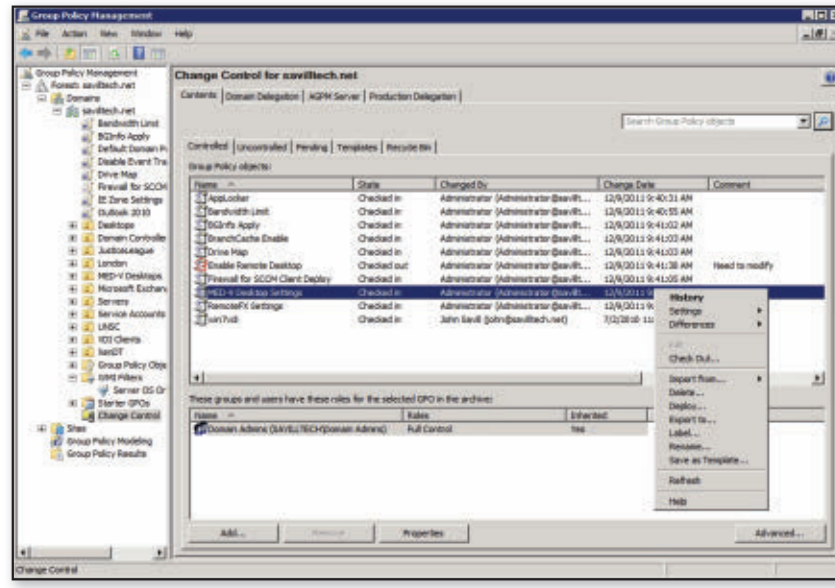


Figure 1: Controlled GPOs and configuration and delegation tabs available with AGPM

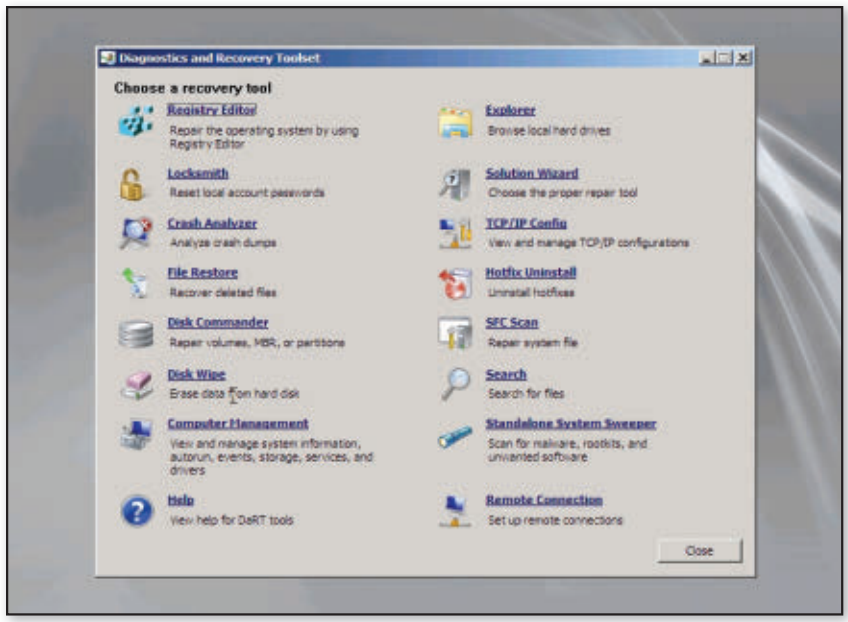


Figure 2: DaRT tools

their arms—because if you lose it and BitLocker needs it, you've lost everything on the disk. One great enhancement that's in the Server 2008 schema and that can be applied to Windows Server 2003 is the ability to automatically save this recovery key as a child object of the computer account in AD. Some additions were made to help the IT Help desk get this key and give to users, but MBAM makes this much nicer by providing a secure web portal that the Help desk can access to give the key to the user. When the recovery key is used, a new one is automatically generated, and a full audit trail is logged, showing when the key was pulled from the database and who pulled it. MBAM uses a small SQL Server database for the recovery key storage and general management, and a SQL Server encrypted database with Transparent Data Encryption (TDE) is used to ensure security of the recovery keys. If you're using BitLocker, you should implement MBAM to get the best management, usability, and compliance within your organization.

DaRT

I doubt that anyone is unfamiliar with Sysinternals, which provides some of the best Windows troubleshooting and administrative tools there are. Sysinternals had a commercial sister site, Winternals Software, that had purchasable solutions for computer management, including great tools to help fix unbootable machines, recover deleted information, and change forgotten local passwords. With Microsoft's acquisition of Winternals, the best of these tools became DaRT, which has been enhanced even further. Although DaRT still supports a machine from CD, DVD, or USB, IT technicians can now also use DaRT over the network and remotely, meaning that a desktop visit is no longer required to help recover a machine.

When a machine boots to DaRT, all the toolset's capabilities, which Figure 2 shows, are available to help resolve a variety of issues:

- Gain full access to both the registry and file system of the OS to recover deleted files or to perform a secure wipe of the disk
- Modify the passwords of local accounts, including administrator accounts
- Perform disk configuration changes, including repairing corrupt volumes and boot records
- View computer information and change settings, including network configuration, services, events, drivers, and AutoRun
- Uninstall hotfixes
- Perform a System File Checked scan to ensure that the correct OS critical files are used
- Scan for and remove malware

DaRT is one of those tools that you should keep on a small USB drive and carry at all times. The toolset is one of those things that you hope you don't need, but when you do need it, you want it quickly on hand. One important note: DaRT is OS-specific. DaRT 7 works with Windows 7 and Server 2008 R2 (DaRT 6.5 also supports Windows 7); earlier versions are also supplied to work with Windows Vista and Server 2008 (DaRT 6) and XP and Windows 2003 (DaRT 5).

Final Thoughts

If you investigated MDOP in the past, you might wonder what has happened to DEM, which allowed the application errors that are typically sent directly to Microsoft to instead be sent to a central internal server, which gave visibility to the errors in the environment and then forwarded them to Microsoft. DEM has been retired from MDOP, though it's still supported per typical Microsoft support timeframes. DEM functionality is now part of System Center Operations Manager (SCOM).

About tools such as DaRT and AGPM, you're likely thinking, "These are great, but I want to use them on my servers. How do I license MDOP on my servers?" You can't license MDOP for servers, but the great news is that you don't need to. If all your desktops are covered by MDOP, you can use DaRT, AIS, and AGPM on your servers as well. If you want to use App-V on your Remote Desktop Session Hosts, there's more good news: App-V for Remote Desktop Session is now part of the standard Remote Desktop Session CAL, so those virtual applications that you create for desktop App-V can be used in your Remote Desktop Session environment as well.

MDOP offers amazing value for any organization, even if you use only one part of the suite. When you're thinking about designing your optimal desktop, you can go that one step further by utilizing MDOP.

InstantDoc ID 141612

John Savill
(john@savilltech.com) is a Windows technical specialist, an 11-time MVP, and an MCITP: Enterprise Administrator for Windows Server 2008. He's a senior contributing editor for *Windows IT Pro* and is currently writing his latest book, *Microsoft Virtualization Secrets* (Wiley).

TOP 10 SharePoint 2010 Configuration Mistakes

Clean up configuration errors and put SharePoint in tip-top shape

by Todd O. Klindt

Microsoft SharePoint 2010 is a complicated beast, with more knobs and levels than you can shake a stick at. It's no wonder we get some of them wrong from time to time. Over the past year and a half of installing SharePoint 2010, I've seen quite a few configuration mistakes, mostly at my own hands. In this article, I'll cover 10 of these errors. I'll explain what the correct configuration is, why it's correct, and how to correct the setting in your farm. If you make all the changes in this article, you'll have the beginnings of a beautiful farm—and one less likely to be ridiculed by your friends and neighbors.

Mistake #1: Scrimping on SharePoint's RAM or Hard Disk Space

If I've seen it once, I've seen it a hundred times: a poor, defenseless SharePoint server working as hard as it can to keep users happy, but having its hands tied because of limited resources. This situation is usually a casualty of aggressive virtualization. Virtualization itself isn't bad, but it must be done intelligently and without sacrificing SharePoint's ability to do its job.

If SharePoint finds itself starved for RAM, it starts shutting off functionality so that it can fit into the available space. It also caches less in the web application pools and recycles those pools more often. Less caching and more recycles result in a degraded end-user experience, as SharePoint must compile the same ASP.NET code over and over. And no one likes unhappy users, not even their mothers.

The solution to this particular issue is easy: Add RAM. Microsoft has published the hardware requirements for SharePoint 2010 at technet.microsoft.com/en-us/library/cc262485.aspx. These requirements state that at the very least, each SharePoint 2010 production server should have 8GB of RAM and a C drive with at least 80GB. In many cases, that won't be enough. If your servers are in production, you can watch their memory utilization to see whether they use the entire 8GB of RAM. If so, they could use more. If your servers aren't yet in production, you can use a variety of load-testing tools to simulate your intended load and see how the servers hold up. For example, you can download the Microsoft Load Testing Kit, part of the SharePoint Administration Toolkit, at www.microsoft.com/download/en/details.aspx?id=20022.

As for your C drive, SharePoint itself doesn't need much space, but Windows does. After all, your server has several years of Windows patches to look forward to. While you're adding drive space to your machine, consider adding a secondary drive as well. This drive is a great place to store all the files that you use when you install SharePoint. All the third-party installation files can go there too. You can also have SharePoint put its log and Search index files on this drive. This approach takes some pressure off the C drive. Happy C drive and happy end users equal a happy SharePoint server administrator.

Mistake #2: Using Virtualized Microsoft SQL Server

As I discussed in mistake #1, virtualization isn't bad. But virtualization allows administrators to make mistakes on a much grander scale. Take virtualizing SQL Server. In the context of SharePoint, this process can be especially painful. The main mistake I see when virtualizing SQL Server is overcommitting the host, be it through RAM, CPU, or drive space. Because everything in SharePoint is stored in SQL Server, if SQL Server is slow, SharePoint is slow.

The obvious solution is to move SQL Server to a physical box, on which it doesn't need to share resources. Moving SharePoint's SQL Server instance is easy, thanks to aliases. I've outlined this process, with pictures, at www.toddklindt.com/sql alias.

If you can't get a physical SQL Server box, then at the very least ensure that your virtualized SQL Server instance has a fighting chance. First, make sure that its virtual drives aren't thin provisioned. I/O is one of the areas in which virtualized SQL Server struggles the most, and thin-provisioned drives exacerbate that problem. Also try to put the SQL Server guests' virtual drives on their own spindles on the host. Doing so should improve I/O by preventing SQL Server from fighting other guests for time with the drives. Finally, you shouldn't allow the virtualization host to overcommit its RAM. If the host must swap to meet its RAM obligations, then it's slowing down SQL Server.

Brent Ozar has recorded a brilliant video on how best to virtualize SQL; you can find it at technet.microsoft.com/en-us/sqlserver/gg429826.aspx. Go get some wine and pizza, invite your fellow SharePoint admins, dim the lights, and watch that video. You'll learn a lot.

Mistake #3: Using the Farm Configuration Wizard

Using the Farm Configuration Wizard was a pretty common mistake when SharePoint 2010 first came out but thankfully has diminished as our familiarization with SharePoint 2010 has increased. The wizard's list of atrocities is long, so I'll just cover some of the better known ones. First, and maybe most heinous, is that all the databases that the wizard creates have nasty globally unique identifiers (GUIDs) at the end of their names. The wizard also creates a content web app, at http://servername, that just doesn't scale well. To add insult to injury, the wizard creates your My Site host on that same web app, at http://servername/my. Finally, the wizard encourages you to create service applications that you might not actually use. It's tough to resist the siren song of those check boxes, I know.

The Farm Configuration wizard leaves its dirty handprints all over SharePoint, and it can be a challenge to clean up all of them. However, a few places can be easily fixed. Start with your web apps. Create a web app for My Site and give it a Fully Qualified Domain Name (FQDN), such as mysites.company.com. Create a My Site host at the web app's root. Use the Windows PowerShell cmdlet Move-SPSite to move any My Site to one content database, and then attach that content database to your new web app. You'll also need to adjust your User Profile Service and tell it about your new My Site location.

> The Farm Configuration Wizard leaves its dirty handprints all over SharePoint.

Next, clean up your service applications. Go through your list of service applications and delete any that you aren't using. You gain no benefit from having a service application that you aren't going to use for another six months. After you've deleted unnecessary service applications, stop the associated service instances (also called *services on server*) that power them. If possible, remove the GUIDs from the service application database names. The technique for completing these tasks varies among service application; the Microsoft article "Rename or Move Service Application Databases (SharePoint Server 2010)" (technet.microsoft.com/en-us/library/ff851878.aspx) has directions for all the service applications. Of course, take good backups before doing any of this.

Mistake #4: Using an Incorrect URL when Creating a Content Web App

Like any relationship, SharePoint and Microsoft IIS have communication problems from time to time. Web app creation is one of those times. SharePoint doesn't tell IIS about changes that you might make to a web app after it's created. For instance, if you create an Alternate Access Mapping (AAM) for a web app in Central Administration, you still need to go into IIS and add the host header for the new address.

The issue is compounded when SharePoint farms that you never thought would need to be accessible from the Internet suddenly need to be accessible from the Internet. Budding SharePoint administrators commonly give their web apps short URLs, such as http://portal, to save users some typing. Of course, that URL doesn't route across the Internet, so the web app needs a fully qualified URL added to its stable of AAMs. Not only is this new URL not written to the IIS host headers, but it's also missing from all the alerts, workflows, and anything else that saves URLs—all those items have the old URL hard-coded in. Because SharePoint didn't write any additional URLs to IIS when they were created, it won't write them to any new SharePoint servers that are added to the farm. Nor will SharePoint write these changes to IIS if the Microsoft SharePoint Foundation Web Application service instance is stopped and started.

This issue might not seem like a big deal, but it has bitten many people at the worst possible time: during an outage. In a few cases, administrators have lost or needed to rebuild a SharePoint server and forgotten about the host headers that they put in manually months earlier. SharePoint is up and going, but when browsing to SharePoint, end users get the blue IIS 7 splash page instead of the SharePoint page that they were expecting. Again, unhappy users usually mean unhappy administrators.

Because SharePoint writes host headers only when a web app is created, you can't *fix* problematic web apps. You'll need to recreate them. That's good news and bad news. The good news is that you won't lose any of the content that your users worked so hard to create. The bad news is that you

will lose all the settings that *you* worked so hard to create.

The first step is to make notes of all your web app settings. In most cases, there won't be many, and you'll be familiar with any changes that you made. Then, detach the content databases from your web app. Keep them safe; you're going to need them. Next, make a copy of the web.config file for that web application. Some settings, such as forms-based authentication (FBA) and BLOB cache settings, are in that file. Finally, go into Central Administration and delete the web app. Tell SharePoint to delete the extra stuff. The scary part is over.

Now, recreate the web app, but do it right this time. First, enter the correct, fully qualified URL in the Host Header box. Do your end users a favor, and put the web app on port 80, as Figure 1 shows. Under the Security Configuration settings, accept all the defaults, even if you're going to use Kerberos or SSL. You can change those settings later, and you want to make sure that the web app works correctly before you apply fancy security settings. Doing so helps in any troubleshooting that you might need to do. Under the Application Pool settings, pick an existing application pool. (I'll explain why in the next section.)

It's important to give your content databases distinct names. You should be able to look at a content database name and know exactly which web app that database goes with. This is another one of those things that doesn't usually seem important but is priceless in a disaster-recovery situation. If the content databases that you detached from the web app before you deleted it didn't have such names, then take this opportunity to right that wrong when you recreate the web app. Give the new content database a good name, then use the PowerShell cmdlet Move-SPSite to move the site collections to that new database. If your content database already has a good name, enter it during the creation of the new web app. If you had multiple content databases, attach the rest after the web app is created.

After the web app is created, you can tweak settings as needed. Most settings can be changed in Central Administration. If you made any changes to the web.config file of the original web app, now is the time to copy those changes to the newly created web.config file. You can use a program such as Notepad++ (notepad-plus-plus.org) to compare the two files. You should now have a well-created web application that you can trust in times of crisis.

Mistake #5: Running Web Apps or Service Apps in Separate App Pools

Web applications and service applications run inside of an application pool, which is a W3WP.exe process that runs on your server. Unless you have reason to do otherwise, you should run all SharePoint web apps inside one application pool; the same goes for the service applications. Running each web app in its own application pool makes inefficient use of the server's memory. Each application pool has a minimum overhead of more than 100MB, and its memory footprint increases as it caches content that's rendered frequently. Figure 2 shows multiple W3WP.exe processes running as sp_webapps, the result of web apps running in separate application pools. We've all experienced SharePoint slowing first thing in the morning because the app pools recycle overnight and need to warm up and cache that content again. Well, multiple application pools mean that the same content is cached multiple times. Most users are impatient. I'm sure that studies would show that they spend the time waiting for SharePoint to respond by thinking of ways to punish us for SharePoint's poor performance.

For service applications, this problem is easy to fix. First, make sure that you have a good service application pool to use. I recommend calling this pool Default SharePoint Service App Pool so that it floats to the top of all your drop-down lists. Use a dedicated sp_serviceapps account (referenced in www.toddklindt.com/serviceaccounts) for the pool's identity. Most service applications allow you to assign them to a new service application pool by modifying their properties in Central Administration. If the option is unavailable there, look for it in PowerShell.

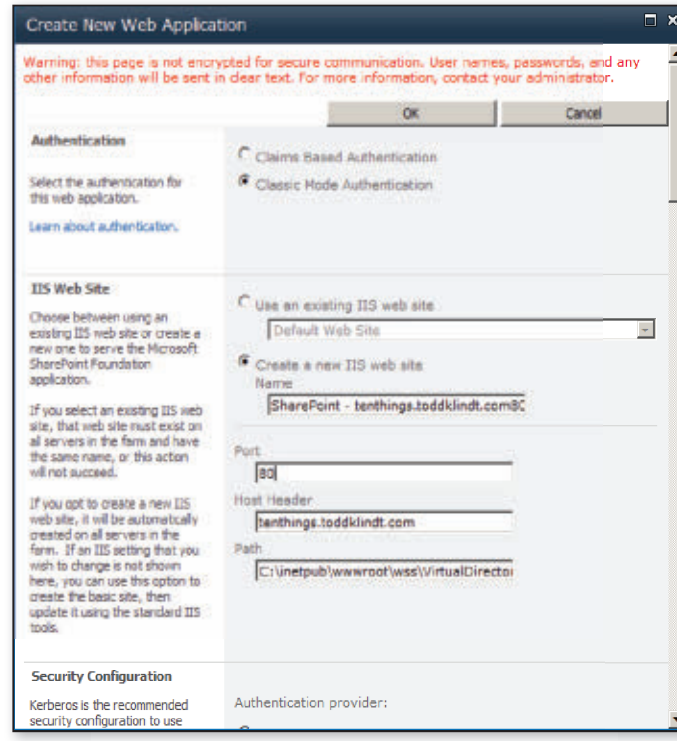


Figure 1: Creating a new web app

w3wp.exe	604	sp_webapps	00	205,008 K	IIS Worker Process
w3wp.exe	940	sp_farm	00	134,716 K	IIS Worker Process
w3wp.exe	5252	sp_serviceapps	00	247,464 K	IIS Worker Process
w3wp.exe	6700	sp_webapps	00	240,340 K	IIS Worker Process
w3wp.exe	7552	sp_farm	00	262,936 K	IIS Worker Process

Figure 2: Result of running web apps in separate application pools

Web applications are a tougher matter. There's no easy, out-of-the-box way to change the application pool that a web app is using. Fortunately, we have PowerShell at our disposal. The steps to this process won't fit in this article, but I outline them in detail at www.toddklindt.com/changeapppool.

Mistake #6: Using One Account for Everything

Security is complicated, and SharePoint doesn't necessarily make it any easier. Using just one account—maybe even the coveted Domain Administrator account—is so easy. We've all done it, even though it's a bad idea. When you use an existing account, you open up SharePoint to several security issues. Anyone who knows the account password can do anything in SharePoint, so you can't separate duties. You also lose the ability to audit who made which changes. And if that common account password is compromised or needs to be changed, you jeopardize SharePoint's uptime as well. Even if you use one dedicated account for SharePoint, you leave yourself vulnerable to attack. If that account is compromised via a security exploit, the bad guys will have access to everything in SharePoint.

To fix this mistake, start by creating the accounts that I outline in the blog post at www.toddklindt.com/serviceaccounts. Add the sp_webapps and sp_serviceapps accounts as managed accounts. Use the techniques that I describe in Mistake #5 to fix your web app and service application accounts. You can change the default content access account for the Search service application at the Search Service Application page. Under Central Administration, Security, Configure Service Accounts, you can change the accounts that other processes use as well. (You can even change the Farm Account there. I've done so in test environments but haven't been brave enough to do it in production.) If you're using the User Profile Service, make sure that your new sp_userprofile account has the correct permissions in Active Directory (AD), and recreate your AD connection in the User Profile Service.

You can also use the steps that I describe at www.toddklindt.com/sp_farm to give an account the correct permissions to administrate SharePoint, without needing to use another highly privileged account.

Mistake # 7: Keeping Default SharePoint Database Settings

When SharePoint creates its multitudes of databases, it makes some bad assumptions. Take the autogrow settings: The database files grow by 1MB at a chunk, almost ensuring that they're going to autogrow with every upload. Not only does this slow down SQL Server (which slows down SharePoint), but it also results in database files that are spread all over your drives in itty-bitty 1MB chunks.

SharePoint also creates most of its databases, notably the Config and Content databases, with the recovery model set to Full. Although this is great if you want to recover data, you must manage the process correctly or those sneaky .ldf files will slowly, methodically fill your hard disk. If you think users get upset when SharePoint is slow because of fragmented databases, you should see how angry they get when SharePoint stops completely because the SQL Server drives are full.

> Autogrow should be a last resort; pregrow your databases so that autogrow is unnecessary.

To fix this mistake, set your databases' autogrow settings in such a way that they don't need to grow frequently. For most farms, I recommend changing the 1MB autogrow to something like 500MB or 1GB. Autogrow should also be a last resort. Someone, either the SharePoint administrator or a dedicated DBA, should pregrow your databases so that autogrow is unnecessary.

Your recovery model setting needs to be consistent with your disaster recovery plans. If you need your transaction logs, make sure you're performing routine log backups to keep those .ldf files in check. If you don't need your transaction logs, then consider switching your databases to the simple recovery model. Doing so will keep your .ldf files from swelling up like a nasty bee sting.

Mistake #8: Not Enabling BLOB Caching

I don't know about you, but I've never heard an end user say, "SharePoint is too fast. Could you get it to respond a bit more slowly?" We all want SharePoint to get files to the users as quickly as possible. However, more often than not, I see SharePoint farms without BLOB caching enabled. BLOB caching is one of the easiest and least expensive ways to improve SharePoint performance. Not only does it help to get files to users more quickly, but it also eases the burden on SQL Server. Everybody wins.

This might be the easiest solution so far: Enable BLOB caching, of course! BLOB caching is actually a function of IIS; SharePoint just takes advantage of it. Therefore, to enable BLOB caching requires a change to each web app's web .config file on each server. Fortunately, the setting already exists and just needs to be enabled. By default, the web.config files are in a directory under C:\inetpub\wwwroot\wss\virtualdirectories. Each web app has a directory and a web.config file. Open one of these files and look for the following line:

```
<BlobCache location="C:\blobcache\14"
path="\.(gif|jpg|jpeg|jpe|jfif|bmp|dib|tif|tiff|
ico|png|wdp|hdp|css|js|asf|avi|flv|m4v|mov|
mp3|mp4|mpeg|mpg|rm|rmvb|wma|wmv)$"
maxSize="10" enabled="false" />
```

To enable BLOB caching, replace "false" with "true" and save the web.config file. You should also move the file to a directory on a drive other than the C drive. The maxSize parameter is measured in gigabytes, with a default of 10GB. If the space is available, you might want to increase this size.

If editing this file in Notepad on all your servers isn't your idea of fun, you can use PowerShell to automate the process. You still need to perform the process on each server, but using PowerShell is quicker and reduces the chances of a mistake. To begin, download the script at www.toddklindt.com/blobcache and save it to a file named blobcache.ps1. This script contains two functions: Enable-SPBlobCache and Disable-SPBlobCache. Each function takes a web app from the pipeline and enables

or disables BLOB caching on that app. The code to enable BLOB caching on each web application in the farm looks like this:

```
PS E:\Install\Scripts> . .\blobcache.ps1
PS E:\Install\Scripts>
  Get-SPWebApplication |
  Enable-SPBlobCache
```

Mistake #9: Not Installing a PDF iFilter

Most organizations have a tremendous number of PDF files in their SharePoint farms, and those files represent a wealth of information. End users want to be able to discover that information by using SharePoint Search. Getting users excited about SharePoint Search is a great way to get them excited about SharePoint in general.

Installing a PDF iFilter is fairly easy. Adobe has a free PDF iFilter that you can install. You can find the download link and detailed installation instructions at support.microsoft.com/kb/2293357. You need to install the iFilter only on those SharePoint servers that run the Search Index role, although installing it on the rest of your SharePoint servers doesn't hurt. If you have a large farm and want to reduce the time needed to index your PDF files, you can use the PDF iFilter from Foxit (www.foxitsoftware.com). This product has better performance than the Adobe iFilter but isn't free.

Again, you can harness PowerShell to make this task easier. Brian Lalancette, creator of AutoSPInstaller (autospinstaller .codeplex.com), wrote a great script that automatically downloads, installs, and configures a PDF iFilter, and this script has become my preferred method. The script is part of a larger package, so I've stripped out the relevant parts and posted them at www.toddklindt.com/PDFSearch. Save that file as pdfsearch.ps1. The file contains two functions: Configure-PDFSearch and Configure-PDFIcon. The former installs and configures the iFilter; the latter adds a PDF icon to the SharePoint interface. As I describe for the script in Mistake #8, install the functions by dot-sourcing the pdfsearch.ps1 file and then executing the function.

Mistake #10: Not Pointing Your SharePoint Servers at Themselves

When SharePoint works, it's magnificent. When it doesn't work, it can be a nightmare to fix. For this reason, anything you can do to ease troubleshooting is time well spent. To that end, I make sure that every server in the SharePoint farm points to itself for all web apps. If I get sporadic reports about SharePoint not responding, I can easily use RDP to log in to each server and try to pull up SharePoint. If this attempt works, then I know that the server is working. If SharePoint doesn't come up, then I know in exactly which Microsoft User Location Server (ULS) logs to look for the relevant errors. No worrying about which web front end the load balancer sent my request to. The quicker you get to the correct log files, the quicker the problem is resolved.

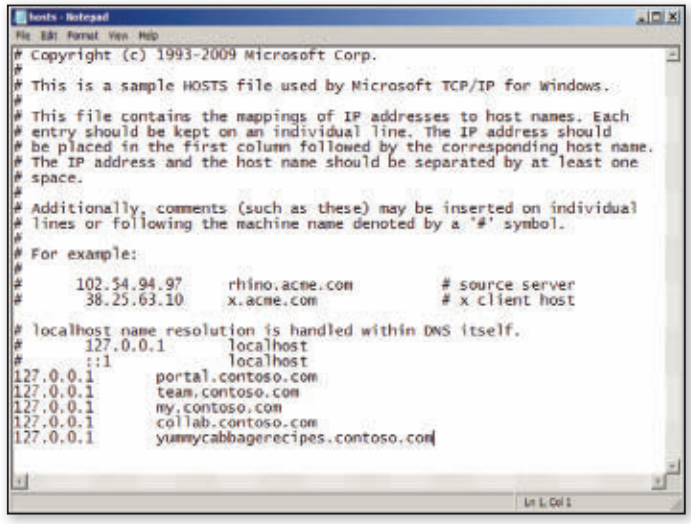


Figure 3: Hosts file in a common SharePoint environment

Pointing your Search indexer at itself has another advantage: It improves performance for your end users. If you don't point your Search server at itself, then when it starts to perform a crawl, it lets DNS do its work and then starts crawling whichever web front end DNS points it to. That server is most likely the same one that's sending pages to your end users. Making the server do double-duty means that everyone waits longer. Pointing the Search server at itself means that your web front end doesn't need to handle that traffic and can get back to doing its #1 job: keeping users happy.

There's a simple fix for this mistake: Open the hosts file (C:\windows\system32\drivers\etc\hosts) on each SharePoint box, and add all the URLs that SharePoint knows about. Point those URLs to 127.0.0.1, which translates to «this computer.» Figure 3 shows how this file looks in a typical SharePoint environment. This approach provides all the benefits that I've mentioned but uncovers a nasty beast: loopback detection. This monster, as well as how to defeat it, is scary and too long for this article, but you can read all about it at www.toddklindt.com/loopback.

As you might have noticed, I'm a fan of using PowerShell to fix these mistakes, and #10 is no different. The script at www.toddklindt.com/edithosts will automatically add all SharePoint's URLs to your server's local hosts file and fix the loopback detection beast in one fell swoop. Is there anything PowerShell can't do?

Everybody Makes Mistakes

There are as many ways to screw up SharePoint as there are grains of sand on the beach. I ought to know; I think I've made them all. Twice. Although you might witness (or make) one or two of the mistakes in this article, the good news is that they can all be fixed. Just follow the instructions here, and your SharePoint farm will be tip-top in no time.

InstantDoc ID 141636

Todd O. Klindt
(todd@sharepoint911.com) is a consultant for SharePoint911 and a SharePoint MVP.

- Novell
- Wilocity
- Atlantis
- Odyssey

Softinventive Lab Offers Elegant Network Inventory

Softinventive Lab announced the release of Total Network Inventory 2, software for computer network inventory. The new version offers greater speed and reliability and can scan computers running MacOS X, FreeBSD, and Linux-like systems just as easily as it could previously scan a Windows device—no pre-installed agents, no preparations, nothing required except the correct password. Developers of Total Network Inventory 2 rebuilt the product from scratch to meet all user requests. As a result, Total Network Inventory has become better in every way, bringing a wealth of new features and possibilities. Among the major improvements are optimized scanning technology, a space-effective storage format, customizable reports, software-accounting and license-tracking tools, and omnipresent live search. For more information, go to www.softinventive.com.

Atlantis Computing Extends to Hyper-V

Atlantis Computing announced Atlantis ILIO for Hyper-V, which runs as a virtual appliance natively on the Microsoft Hyper-V hypervisor for deployment with Citrix XenDesktop. Atlantis ILIO is the first storage-optimization solution that can be deployed on any server with any storage and on any of the three major hypervisors: VMware vSphere, Citrix XenServer, and Microsoft Hyper-V. The Atlantis ILIO software virtual appliance allows customers to reduce the cost of their VDI implementations by cutting the amount of storage normally required and enabling the use of lower-cost storage options as part of any desktop virtualization project. Atlantis ILIO also makes virtual desktops run faster than PCs to ensure user acceptance and enables security measures to be deployed without affecting the number of users per server. For more information, see www.atlantiscomputing.com.

PRODUCT SPOTLIGHT

Novell ZENworks Application Virtualization 9

Novell announced the immediate availabiity of Novell ZENworks Application Virtualization 9, which leverages a unique approach to application harvesting that enables enterprise IT staff to tap into a library of trusted resources and find the best stored version to build the necessary virtual application dynamically. By harvesting work that has already been done, IT users can scan a target endpoint and quickly build a set of needed virtual applications, saving time and ensuring quality. ZENworks Application Virtualization 9 includes access to a large number of prebuilt templates for building virtual applications based on tested and optimized application configurations. These web-based templates provide IT administrators with access to a central repository that includes the most up-to-date versions of common applications. Building applications using templates greatly reduces the manual labor necessary to configure virtual applications, and web-based access eliminates the need to upgrade the version of ZENworks Application Virtualization each time an application needs to be updated, thereby reducing IT labor and costs.

Additional customer benefits of Novell ZENworks Application Virtualization 9 include offline streaming support, providing fast adaptive application streaming and the ability for streaming applications to be executed without a persistent web connection; "juke-boxing," providing the ability to launch individual products from within a single application stream for suite applications; and application control, ensuring that IT can maintain compliance with its license agreements. For more information about Novell ZENworks Application Virtualization 9, visit www.novell.com/zav.

triCerat Virtualizes User Profiles

triCerat released a new version of its Profile Acceleration Technology. PAT 1.1 improves the way OSs access user profiles by virtualizing them, not altering them. Users will immediately experience the difference of speedy logon and logout times, reduced network utilization, decreased profile corruption, offline access to profile data, and ultimately increased productivity. The new version of PAT supports increased mobility with offline mode for laptops and provides an improved UI for a quick and seamless installation and implementation. PAT doesn't change existing user profiles, so there's no learning curve. Regardless of your environment's size, profile virtualization will provide newfound resiliency, efficiency, and ease of use to your system. For more information, see www.tricerat.com.

Sourcefire Brings Increased Awareness, Automation to Threat Prevention

Sourcefire announced the Sourcefire Next-Generation Firewall (NGFW). Building on Sourcefire's Next-Generation IPS (NGIPS) technology and leveraging its FirePOWER platform, NGFW combines IPS threat prevention, integrated application control, and firewall capabilities into a high-performance security appliance. By combining NGIPS and NGFW, Sourcefire has created the first enterprise firewall solution with

comprehensive enterprise visibility, adaptive security, and advanced threat protection. Applying its Agile Security vision to the emerging NGFW market, Sourcefire is delivering a context-aware and adaptive NGFW solution to offer its customers superior network protection and control without compromise. For more information about Sourcefire, please visit www.sourcefire.com.

Wilocity to Deliver Multi-Gigabit Wireless

Wilocity announced that it will deliver the world's first multi-gigabit wireless system based on the newly completed and ratified WiGig 60GHz standard in mid-2012. At CES, Wilocity showcased live WiGig applications in action, including home, office, and on-the-go demos of high-speed docking, networking, and HD video that are 10 times faster than existing Wi-Fi data rates. The company's unique tri-band solution enables users to connect at whatever band offers the best available performance, delivering multi-gigabit data rates at 60GHz while maintaining compatibility with hundreds of millions of existing Wi-Fi products in the 2.4GHz or 5GHz bands. "Wilocity has the ingredients to kick-start WiGig as the next major breakthrough in mobile information delivery and transfer," said Filomena Berardi, senior analyst at IMS Research. For more information about WiGig, please go to www.wilocity.com.

Odyssey Offers Mobile Device Management for Kindle Fire

Odyssey Software announced that its award-winning Athena software provides premium support for Amazon's Kindle Fire. "Managing the influx of employee-owned (or BYOD) devices brought into the corporate environment is a tremendous challenge for IT administrators," said Mark Gentile, CEO of Odyssey Software. "Millions of Kindle Fire devices were sold in December, and many of these will find their way onto corporate networks even though they were not purposefully designed for use in the enterprise. To address some of these challenges, we strongly recommend that all BYOD devices be approved and enrolled in a mobile device management (MDM) program before allowing employees to connect to the corporate network." Athena's premium support for the Kindle Fire includes enabling live access to devices plus passcode reset, lock, and wipe functions for remote assistance; reporting detailed hardware, software, network, and device health information; setting passcode policies; and deploying applications, documents, and media. More information is available at www.odysseysoftware.com.

Paul's Picks

www.winsupersite.com

SUMMARIES of in-depth product reviews on Paul Thurrott's SuperSite for Windows

Lenovo IdeaPad YOGA Flip (Preview)

PROS: Unique design offers both laptop and tablet form factors; 8 hours of battery life; high resolution (1600 × 900) screen

CONS: Heavier and bulkier than a tablet

PRELIMINARY RATING: ◆◆◆◆◇

RECOMMENDATION: Lenovo describes the IdeaPad YOGA Flip as "the industry's first multi-mode notebook." Its 360-degree, flip-and-fold screen design lets it function as a normal laptop computer, or the screen can be flipped around, like a convertible laptop. Or it can be used in a unique new tent mode, in which the the device acts as its own stand in a multi-touch tablet form. Lenovo says the YOGA Flip supports four separate usage modes. Detractors say that its 3.1 pounds can't compete with iPad and Android tablets, but that's missing the point: The YOGA Flip is a laptop first, tablet second. Looks good to me.

CONTACT: Lenovo • www.lenovo.com

DISCUSSION: www.winsupersite.com/article/windows8/windows-8-lenovo-ideapad-yoga-split-141846

Nokia Lumia 900

PROS: Innovative design; superior screen; LTE 4G capabilities; unique Nokia-only apps

CONS: Only available on AT&T, at least temporarily; low 800 × 480 screen resolution

PRELIMINARY RATING: ◆◆◆◆◇

RECOMMENDATION: The Lumia 900 has the same beautiful polycarbonate casing as the Lumia 800, but in a slightly bigger package (in blue/cyan and black versions). Its AMOLED screen is superior to the one on the Lumia 800, but retains the same 800 × 480 resolution, as mandated by Windows Phone. It has an excellent 4G LTE antenna for compatibility with AT&T's network. It has a large 1830mAH battery for longer-lasting performance. And best of all, its camera offers Carl Zeiss optics, a large aperture (f2.2), and a wide-angle focal length (28mm) for what should be high-quality images even in low-light conditions. This is the premier Windows Phone. I'm buying one March 18, when it becomes available in the US.

CONTACT: Nokia • www.nokia.com

DISCUSSION: www.winsupersite.com/article/windowsphone75/nokia-lumia-900-preview-141872

InstantDoc ID 141964

REVIEW

VMware vCenter Protect Essentials Plus

VMware vCenter Protect Essentials Plus (formerly known as Shavlik NetChk Protect) is primarily an update compliance tool that lets you determine whether your Windows computers are up-to-date with patches. Its capabilities go beyond what's available in tools such as the Microsoft Baseline Security Analyzer (MBSA). For example, you can determine whether updates are missing from not only Microsoft apps but also third-party and custom apps. Detecting missing updates for third-party apps is important because third-party apps rather than Microsoft apps are now the dominant malware vector.

You can also do the following with vCenter Protect Essentials Plus:

- Perform scans and deploy updates with or without an agent.
- Deploy updates to computers for Microsoft, third-party, and custom apps.
- Roll back update deployment for Microsoft, third-party, and custom apps.
- Deploy and monitor an anti-malware agent (included with the Plus edition; available as an add-on for the standard edition).
- Reduce power consumption, shut down, restart, or wake managed computers on a scheduled basis (included with the Plus edition; available as an add-on for the standard edition).
- Determine what hardware and software has been installed on physical and virtual clients (not available in the standard edition).
- Scan by domain, organizational unit (OU), computer name, and IP address range.
- Easily execute Windows PowerShell scripts on remote machines with the ITScripts feature (not available in the standard edition).
- Quickly connect to target machines via RDP integration and credential storage.
- Create custom reports that let you analyze data on missing updates, update deployments, and malware threats.
- Scan and update offline virtual machines (VMs), provided that vCenter Protect Essentials Plus has access to the VM host.

As Figure 1 shows, the product's console has an interface that will be familiar to users of Microsoft's System Center suite.

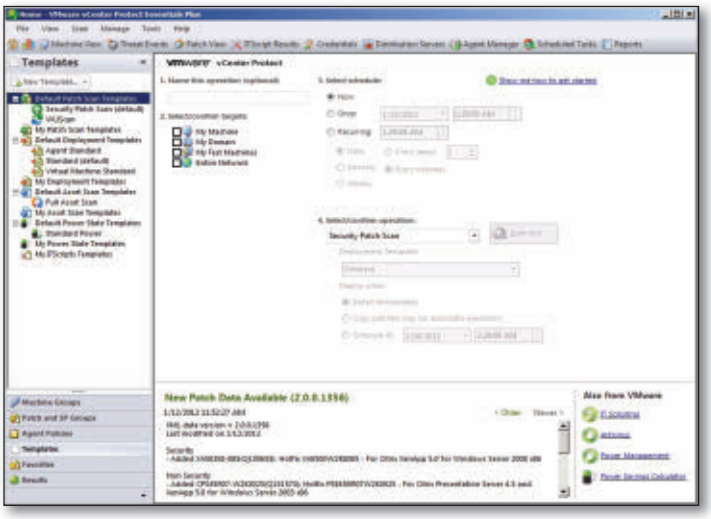


Figure 1: The vCenter Protect Essentials Plus console

The console's layout lets you quickly discover functionality without having to dig through an arcane menu structure.

An important feature is the ability to scan for missing updates to custom and third-party apps. You use the Custom Patch File Editor to assist with this functionality. It helps you use patch files to generate an XML file that lets you find unpatched machines and deploy the needed updates.

vCenter Protect Essentials Plus requires SQL Server 2005 Express Edition or later. The installation routine connects to the Internet and automatically downloads SQL Server 2008 R2 Express if you don't have an available SQL Server instance. When installing my review copy, I had some problems with this aspect of the installation. The routine didn't detect the SQL Server Express instance on my machine. I ended up deploying a separate SQL Server 2008 R2 instance.

The product supports client computers running Windows 2000 and later. Scanning offline VMs requires that you're using VMware virtualization software.

vCenter Protect Essentials Plus allows a substantial amount of customization in how you scan for and deploy updates. You can use machine groups for differentiated missing update detection and deployment. You can also configure Patch Scan templates, which let you be selective about looking for missing updates. If you're in the market for a versatile tool that can manage update compliance for Windows OSs as well as Microsoft, third-party, and custom applications but you don't want the expense of deploying a product such as Microsoft System Center Configuration Manager (SCCM) 2012, check out vCenter Protect Essentials Plus.

InstantDoc ID 141960

VMware vCenter Protect Essentials Plus

PROS: Quickly determines if computers are missing important OS and application updates

CONS: Encountered problem with automatic configuration of SQL Server Express

RATING: ◆◆◆◆◆

PRICE: Starts at $57 (Plus edition) or $38 (standard edition) for the term license and 1-year production support (24 x 7 for Severity 1 issues); starts at $53 (Plus edition) or $35 (standard edition) for the term license and 1-year basic support (12 hours per day Monday through Friday)

RECOMMENDATION: vCenter Protect Essentials Plus is a good choice for organizations that are looking for a tool to manage update compliance for Windows OSs as well as Microsoft, third-party, and custom applications without the expense of deploying a product such as SCCM 2012.

CONTACT: VMware • 800-690-6911 or 877-486-9273 • www.shavlik.com

Orin Thomas | orin@windowsitpro.com

Penton Marketing Services
WE KNOW YOUR CUSTOMERS
powered by eyetraffic

Do you know what is being said about your company online?

DO YOU KNOW WHAT IS BEING SAID ABOUT YOUR COMPETITION?

We do.

Do you have time to warm prospects towards a sale?

DO YOU HAVE THE RESOURCES TO RESPOND QUICKLY TO PROSPECT BEHAVIOR?

We do.

Announcing, smart marketing for the technology industry.

We target the tough questions.

Windows IT Pro
SQL Server magazine
SharePoint Pro CONNECTIONS
DevProConnections
SystemiNetwork

Penton Marketing Services offers a full range of marketing products that leverage our deep industry knowledge and customer relationships. From product launch to the final sale—put our years of experience to work for you.

FOR MORE INFORMATION:
PentonMarketingServices.com
800 553 1945

REVIEW

SolarWinds User Device Tracker 1.1

SolarWinds User Device Tracker (UDT) 1.1 is a network port–tracking application designed to be used as a standalone program or with other SolarWinds products, such as Orion Network Performance Monitor. UDT scans ports on routers and switches, returning information on the attached devices so you can run searches against the results. Despite the product's name, UDT doesn't display who is logged on to a device. However, in version 2.0 (which is due for release in first quarter 2012), you'll be able to map Active Directory (AD) users to PCs.

The primary use for UDT is to detect rogue devices on a network and help determine their physical location. You might need to track down a wireless router or a PC infected with a virus that's causing network performance problems. As Figure 1 shows, you can set up watch lists to track when devices are attached to the network. You can also keep track of port utilization over time so you can plan for future capacity upgrades.

UDT uses SNMP to collect information and is compatible with any device that has a standard MIB. As part of the first year's maintenance contract, SolarWinds adds support for devices that UDT doesn't recognize.

Figure 1: Using watch lists to track when devices are attached to the network

Installing UDT

UDT relies on the SolarWinds Orion framework for the back-end infrastructure (most of the company's products are based on this framework), a web GUI, and a set of management tools. UDT requires Windows Server 2003 or later, IIS, and SQL Server. When I launched the UDT installer, it informed me that not all the required components of IIS 7 were present and offered to automatically install the missing modules. I wish all installer routines were so user friendly. A configuration wizard then quickly connects the Orion framework to your SQL Server database and installs some additional components.

Working with UDT

When launching UDT for the first time, you can add network devices manually or run network auto-discovery. Basic information is displayed for each node, such as its CPU load, memory usage, and Internetwork Operating System (IOS) version. The Orion framework can also collect syslog data. After a node has been added, a wizard takes you through detecting ports. UDT then displays what's connected to them.

UDT's power lies in its ability to not only search live data but also run searches against historical port information. You can search by IP address, subnet, host name, or MAC address. For convenience, first and last seen information is shown for each device and search results can be exported as comma-separated value (CSV) or PDF files.

Watch lists are easy to set up. If you want to receive an alert when a device on your watch list attaches to the network, you use the Advanced Alert Manager application to add the alert. Alerts can trigger a variety of different actions and, once created, can be edited from the web interface. UDT provides a variety of built-in reports that can be scheduled and sent by email. A separate application, Orion Report Writer, is included for customizing reports.

The web GUI is very intuitive and easy to navigate, letting you drill down and find the information you need. If you have geographically dispersed sites, the home page can be set up to display a network map so you can locate equipment easily.

An Elegant Addition to the SolarWinds Family

At a fraction of the cost of other port-tracking solutions, UDT does what it says on the box. Equally important, it's easy to set up and use. Medium to large enterprises should consider deploying UDT if they're in the market for a more complete network management solution. If you want to see the product in action without installing it in your environment, you can view an online live demo at oriondemo.solarwinds.com.

InstantDoc ID 141324

SolarWinds User Device Tracker 1.1

PROS: Ease of use; price; integration with SolarWinds network management products

CONS: Expensive for small-to-midsized businesses (SMBs)

RATING: ◆◆◆◆◇

PRICE: Starts at $1,795 for 2,500 ports

RECOMMENDATION: When integrated with Orion Network Performance Monitor or other SolarWinds products, this product makes a useful addition to a network management suite.

CONTACT: SolarWinds • 866-530-8100 • www.solarwinds.com

Russell Smith | rms@russell-smith.net

Acronis Backup & Recovery

Backups have sure changed over the years. Just a few years ago, the way we backed up physical servers was to copy the data to tapes. Now we can back up to disks and even to someone else's data center (what some people call "the cloud"). We also have to think about how to back up and recover virtual machines (VMs) and non-Windows OSs, such as Linux. Acronis Backup & Recovery 11.0 can help you with all your backup needs.

Using Acronis Backup & Recovery, you can back up local and remote physical computers running Windows 2000 with SP4 or later (with the exception of Home Editions of Windows client OSs) or Linux with kernel 2.4.20 or later. The latter includes Red Hat Enterprise Linux 4.0 and later, Ubuntu 9.10 and later, Fedora 11.0 and later, SUSE Linux Enterprise Server 10.0 and later, Debian 4.0 and 5.0, and CentOS 5.0. If you have a virtual environment that you would like to back up directly, Acronis Backup & Recovery supports Microsoft Hyper-V, VMware Infrastructure 3.5, and VMware vSphere Hypervisor (formerly VMware ESXi) 4.0 and later. Supported file systems include FAT16, FAT32, NTFS, Ext2, Ext3, Ext4, ReiserFS 3, ReiserFS 4, XFS, JFS, and Linux Swap.

Installation

Acronis Backup & Recovery comes in a 1GB installation file. Although the installation took some time to complete, it ran flawlessly and was completely hands-off. It even took care of all the prerequisites, such as installing SQL Server 2005 Express.

After the installation was complete, I opened up the management console and proceeded to set up a backup schedule for the domain controller (DC) in my test domain. The first step was to install the backup agent on the remote DC. However, the remote installation of the agent failed initially, because the DC didn't have ports 9876 and 25001 open. After I opened up those two ports, the agent installed.

You have many installation options for the agents as well as the main program. The most obvious method is to double-click the application executable and walk through the setup routine. However, you can also install the software remotely through a scripted method (e.g., using an .mst file in Windows, using the command line in Linux) or by using Group Policy. I like the Group Policy method. You simply create a Group Policy Object (GPO) for the parent *Servers* organizational unit (OU) to ensure that every new server added to the domain has the correct Acronis components.

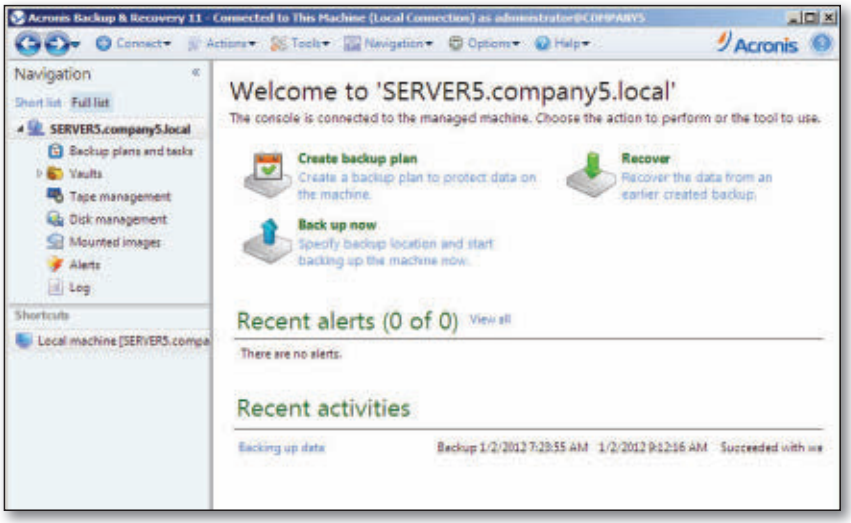


Figure 1: The Acronis Backup & Recovery management console

> The installation took some time to complete but ran flawlessly and was completely hands-off.

Backups

The heart of Acronis Backup & Recovery is the Management Server component. It's used to configure and manage the backups on the network. The first step in backing up a network is to create a backup plan in the management console, which Figure 1 shows. This process involves completing four sections.

What to back up. In this section, you identify which servers or services need to be backed up. This includes entire volumes on servers. You can't choose individual files to back up, but you can choose specific files or file types to exclude, such as hidden or system files and folders, or files with a specific extension (e.g., files with an .mp3 extension).

Where to back up. Acronis Backup & Recovery offers a wide choice of target locations to store your backups. In addition to tape drives (Advanced version only), backups can be stored in a local folder on a hard drive, a remote network share, an FTP or SSH File Transfer Protocol (SFTP) server, a storage node, or online via Acronis Online Backup.

If you want to kick the tires of Acronis Online Backup, you can try it before you buy it. You can back up as much as 1TB of data for free for 60 days. The registration process is quick and doesn't require a credit card. In just a few minutes, I was able to back up my test server online. If the online backup (or restore) fails due to a communication problem, Acronis Backup & Recovery will try again every 30 seconds. It will do this five times by default, but this parameter can be changed.

How to back up. In this section, you specify the type of backup (i.e., full,

Eric B. Rux | ebrux@whshelp.com

ACRONIS BACKUP & RECOVERY

incremental, or differential). You also configure the schedule, retention rules, and validation rules in this area.

Retention rules can be set to either keep the backups indefinitely or delete the backups that are older than a specified number of days. If you need a more comprehensive backup scheme, older backups can be moved to another medium. For example, the backups can be initially stored on disk drives, then later migrated to tapes or an offsite location.

If you're going to store the backups online at the Acronis data center, you might want to perform an "initial seeding" backup first. This is done by performing a full backup of the server on an external hard drive, then mailing the drive to Acronis via FedEx or United Parcel Service (UPS). This saves time because the initial full backup is usually very large and can take a long time to copy over the Internet. The subsequent backups are incremental. The charge for the Initial Seeding service is on a per-server basis (starting at $100 for 2TB of data per server).

Plan parameters. There isn't enough space to go into the details of every option you can configure in the *Plan parameters* section, so here are some options that stand out:

- *Archive protection.* You can set a password and even encrypt the backup for additional protection.
- *Compression level.* You can set the compression level to None, Normal, High, or Maximum.
- *Disaster recovery plan.* If you enable this feature, a disaster recovery plan is emailed to the individuals who will be responsible for performing a disaster recovery. According to the user guide, the disaster recovery plan "contains a list of backed up data items and detailed instructions that guide a user through a process of recovering these items from a backup."
- *Fast incremental/differential backup.* Instead of determining whether a file has changed based on the file's contents, you can use the file's size and the date and time when the file was last modified to determine if a file has changed.
- *Pre/Post backup commands.* You can run a script or program before or after the backup has started or completed.
- *Sector-by-sector backup.* You can use this backup method when you need to back up a file system that isn't supported.

There are other options as well, but I found them to be common to most backup software, such as options to enable Microsoft Volume Shadow Copy Service (VSS) or configure email notifications.

Restores

A backup is only as good as the restore. In addition to the basic restore features, Acronis Backup & Recovery has a unique capability called Universal Restore. This functionality lets you restore a backup to dissimilar hardware—a real-world possibility if your company falls victim to a fire, theft, or flood.

As with all backup and recovery software, be sure to test the backups regularly.

It's also possible to restore from "bare metal." Instead of installing a base OS and recovery software on the new hardware before restoring the backup, Acronis backups can be applied to fresh hardware right out of the box. A wizard walks you through creating either a Linux-based or Windows Preinstallation Environment (Windows PE)–based bootable media for a floppy drive, CD/DVD drive (.iso file), Preboot Execution Environment (PXE) server, or Remote Installation Services (RIS) server. Acronis supports Windows PE 3.0, 2.1, and 2.0. These boot environments must be downloaded and installed separately before the wizard can create this type of bootable media.

Minor Gripes

As well as Acronis Backup & Recovery is put together, I did experience some strange behavior on occasion. For example, clicking Create Folder while in the online backup storage area generates an error message noting that the operation isn't supported. To add to the frustration, the knowledge base link provided in the error message takes you to a page that states, *We are sorry. There is no information about this error available now.* It would make more sense to simply remove the Create Folder button when in the online backup storage area of the application.

Final Thoughts

I was impressed with how easy it was to set up Acronis Backup & Recovery. After the product was installed, I was able to quickly configure a robust backup and recovery scheme. The interface is intuitive. The online backup's integration into the interface is seamless and works well (with the exception of the strange error messages that I just mentioned). Overall, I found the product to be easy to use. As you evaluate backup software, be sure to add Acronis Backup & Recovery to your list.

As with all backup and recovery software, be sure to test the backups regularly. The only way to ensure that the backup software is working properly is to perform an actual restore. This might take additional hardware, but it'll be worth it if you ever need to restore a server. Remember that backups always work; restores never do. If you're not testing your backups regularly, you might find out that the backups aren't working after it's too late.

InstantDoc ID 141826

Acronis Backup & Recovery

PROS: Simple to set up and understand; multiple backup target options (e.g., tape, hard drive, cloud)

CONS: Some error messages aren't clear or send you to knowledge base articles that don't exist; no "agent only" price (each server must have a full license at full cost)

RATING: ◆◆◆◆◇

PRICE: $853 (Standard) or $1,399 (Advanced); one-year subscription to Acronis Online Backup starts at $49 per workstation to back up 250GB of data, $499 per server to back up 1TB of data, and $1,199 per VM to back up 2TB of data

RECOMMENDATION: If you have a hodgepodge of Windows, Linux, and VMs that need to be backed up by one product, Acronis Backup & Recovery delivers.

CONTACT: Acronis • 877-669-9749 or 781-782-9000 • www.acronis.com

HP E5000 Messaging System for Microsoft Exchange Server 2010

The HP E5000 Messaging System for Microsoft Exchange 2010 is part of a new range of appliances created as part of the Microsoft-HP alliance. There are appliances for messaging, business intelligence (BI), data warehousing, and database consolidation. The general aim of these appliances is to enable customers to shorten the deployment cycle while implementing a solution that follows best practices.

The HP E5000 series of appliances lets customers experience the benefits of Exchange Server 2010 (e.g., large mailboxes, archiving, high availability) without the need to fully scope and scale a custom solution. Sizing an Exchange deployment is typically a complex undertaking that requires careful analysis of the many factors built into a user profile. In the HP E5000 series, HP does that sizing for you. It provides a variety of models that cater to small and mid-sized deployments. The HP E5300, HP E5500, and HP E5700 appliances support up to 500 users, 1,000 users, and 3,000 users, respectively, with mailboxes ranging from 1GB to 2.5GB in size. You can add additional units, taking deployments up to 15,000 users. The appliances can also be used in branch offices of large enterprises, providing an easy-to-deploy and uniform way of supporting remote sites.

Although HP has done all the sizing for you, it's important to note that you need to stick to the usage profile outlined. For example, if you start adding BlackBerry or other devices that create an additional load on the Exchange server, you might have to consider reducing the number of supported users. For complex scenarios, you might consider discussing your deployment with an Exchange consultant to see whether an appliance solution or a traditional (and more scalable) hardware solution makes more sense.

It's also important to note that once an HP E5000 appliance is up and running, it's not really any different than any other Exchange server in your organization in terms of management. For this reason, I'll spend more time discussing how to install and configure the appliance than on how to manage it.

Figure 1: The HP E5300 model

Installing and Configuring the System

The first thing that will strike you when you receive your HP E5000 appliance is just how large and heavy it is. Although it doesn't take up much space in a rack (only 3U when used without additional storage shelves), the unit is very deep. As such, it's worth checking the specifications and your existing racks to make sure it will fit.

I tested the HP E5300 unit, which Figure 1 shows. It's comprised of a pair of ProLiant c-Class blades, which sit alongside a storage unit that can hold up to sixteen 3.5" Serial ATA (SATA) or Serial Attached SCSI (SAS) drives. The HP E5300 requires only 12 drives to support the 500 users allowed. These drives store the Exchange data. In each blade, there are two small form factor drives, which are used for OS and application installation. As part of the setup process, you'll end up with the storage carved up between the two blades. Each blade forms part of a database availability group (DAG) and runs the three core Exchange server roles (i.e., Mailbox, Client Access, and Hub Transport). This gives you a highly available deployment of sorts, although to be complete, you'll need a hardware load balancer to provide high availability for the client connections.

I used the HP quick start documentation to guide me through the installation process. After setting up the rack and cables, you begin the configuration process by setting your administrative workstation to a specific IP address on the same subnet that comes preconfigured on the appliance. Afterward, you log on to the Environmental Monitoring Unit (EMU—think of this as the chassis and storage subsystem) and the Integrated Lights-Out (iLO) cards (which give you a console KVM connection to the blades themselves). In general, I found the quick start guide useful and clear. However, it didn't mention one item that caused a problem: the need for a 1GBps or higher switch. It turns out that the NICs are 10GBps and will only negotiate down to 1GBps and no lower. After I found a suitable switch, the install process proceeded nicely.

After you've configured the relevant network and password settings, you can begin to configure the first blade. The blades come with Windows Server 2008 R2 SP1 pre-installed, so you just need to run a wizard to complete the OS setup. Once complete, the HP Configuration Wizard automatically loads and connects to the EMU to set up the storage options and run diagnostics, among other things. Another wizard then guides you through configuring a server OS administrator password, network settings, and domain and computer name settings. Afterward, you must manually run the Schema preparation using the Exchange setup.com program in the normal way for Exchange 2010, but all the relevant files are already loaded on the server.

With the basics completed, the HP E5000 Messaging System Quick Deployment tool starts up and takes you through the deployment of Exchange 2010. If

Nathan Winters | nathan@clarinathan.co.uk

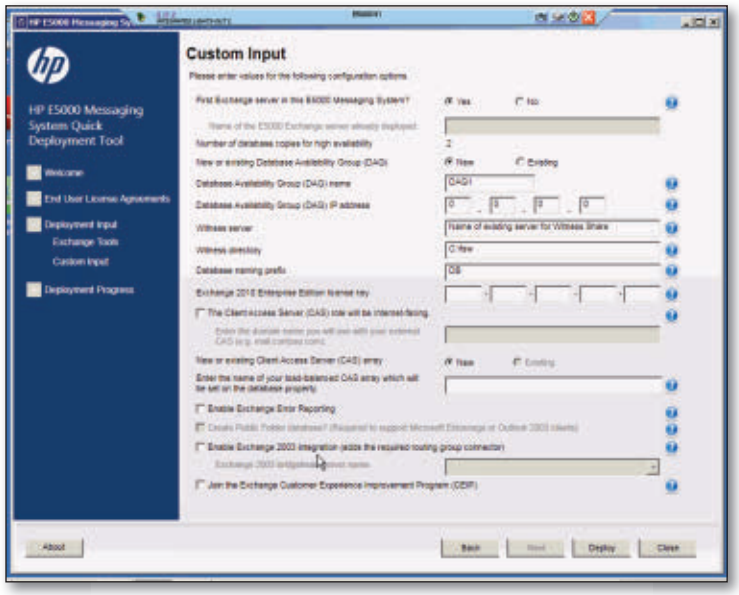


Figure 2: The HP E5000 Messaging System Quick Deployment tool

you're familiar with deploying Exchange, you'll recognize all the usual questions. As Figure 2 shows, the questions have simply been laid out one on page, with information to guide you through the choices. I must admit, though, that the information could be better. There were a couple of elements that weren't clear. For example, I already had an Exchange 2007 server in my predominantly Exchange 2003 organization. Therefore, this server had the routing group connector configured and the public folder replicas on it. The wizard didn't pick up on this and still allowed me to try to set up a connector to the new Exchange 2010 server, which then failed and essentially broke the wizard. After a call to HP support and some messing around in the registry, I got back on track. So, although this page is nice and allows you to enter most of the basic configuration information that Exchange needs (including the information needed to create or join a DAG), there are some pitfalls.

After I resolved the problems and got Blade 1 installed, I repeated the process for Blade 2, except this time I joined the DAG created previously.

Aside from the deployment wizards, there are a few other nice touches. For example, before the deployment, you have the chance to run the Exchange Pre-Deployment Analyzer and JetStress to validate the storage. After the deployment, you can run the Exchange Best Practices Analyzer to validate the system.

Managing the System

After the system is deployed, HP provides the capability to keep the hardware up-to-date with the latest firmware. However, the Windows and Exchange software updating is entirely up to you. As such, you'll still need to manage patches, antivirus updates, and antispam updates the same way you would manage them in a standard Exchange deployment. In fact, aside from some HP tools built into the Server Manager window, there's nothing to distinguish this deployment from a standard Exchange deployment. The built-in tools give you an overview of the system's health through views of the hardware state and services state, as well as some basic information on the state of Exchange. For example, in the standard Server Manager interface, you'll find a node named *System and Network Settings* in the HP E5000 System Manager area. It gives you a page full of links to access the HP installed utilities, such as the HP Array Configuration Utility, HP Lights-Out Configuration Utility, and HP System Management Homepage. The latter provides a window into the hardware of the system, much like you get with any HP server.

On the HP E5000 System Manager node, you can get access to reports on the status of Exchange. The reports are essentially precanned PowerShell commands whose results are shown in the Server Manager window. Among other things, you can see the status of the mailbox databases and high-availability copies as well as reports on mail queues and numbers of active users being served by the Client Access servers.

Some administrators might feel that HP and Microsoft should have included Microsoft Forefront Online Protection for Exchange (FOPE) and a management console that reports on key indicators with the appliance. However, other administrators might be pleased that they can manage the appliance just like any other Exchange server.

Well Worth Evaluating

The HP E5000 series is a great system to get an Exchange deployment up and running quickly. If the prepackaged units fit your user population needs, then all will be well. If not, consider using a traditional Exchange deployment instead. The appliances are easy to configure, and HP support is generally helpful once you reach the right department. The HP E5000 series is well-worth evaluating if you're planning a small or mid-sized Exchange deployment or you need a simple yet efficient branch office solution. *Windows IT Pro* contributing editors Paul Robichaux and Tony Redmond helped HP create a series of videos about the HP E5000 series if you'd like more information about the appliance. Go to www.youtube.com/hewlettpackardvideos and search on E5000.

InstantDoc ID 141862

HP E5000 Messaging System for Microsoft Exchange Server 2010

PROS: Quality hardware; easy installation; good support

CONS: Occasional quirks in the deployment wizard; requires hardware load balancer for a highly available deployment

RATING: ◆◆◆◆◇

PRICE: $36,677 for HP E5300

RECOMMENDATION: The HP E5000 series is well worth investigating for small, medium, and branch office deployments of Exchange 2010.

CONTACT: HP • 650-857-1501 • www.hp.com

Mac Virtualization Products

Parallels Desktop 7 for Mac vs. VMware Fusion 4.1

by Jeff James

It's an undeniable fact that more Apple products are finding their way into the workplace. The wildly successful iPhone and iPad have been steadily making inroads into the enterprise. According to a January 2012 Forrester Research survey of more than 10,000 information workers, more than 21 percent of them are using Apple products in the workplace. Apple's global share of the PC market has also been increasing over the past few years, reaching a high of 5.2 percent of worldwide computer sales, according to an analyst cited by GigaOM.

The result of Apple's inroads into the workplace is that more IT pros will be tasked with supporting Mac users, so having a way to run virtualized Windows applications on a Mac can come in handy. For that reason, I decided to take a look at Parallels Desktop 7 for Mac and VMware Fusion 4.1, the latest versions of the two leading hardware virtualization products available for Macs.

My test machine for this comparative review was a 15" MacBook Pro running OS X 10.7.2, with 4GB of RAM, a 2.53GHz Intel Core 2 Duo processor, a 300GB hard drive, and a discrete NVIDIA GeForce 9400M graphics chipset. Astute readers might recognize this MacBook as the same test machine I used to compare VMware Fusion 2.0 and Parallel Desktop 4.0 in the comparative review "VMware Fusion vs. Parallels Desktop" (September 2009, InstantDoc ID 102578). I specifically wanted to use the same machine to see how well both products have improved after nearly three years of ongoing refinement and improvements. I'm happy to say that both products have improved significantly since then, but which one has the edge? Let's find out.

Parallels Desktop 7 for Mac

Parallels Desktop was first released in 2006 and has been steadily updated since then. The latest release, Parallels Desktop 7, is benefiting from those years of updates and revisions. Installation is slick and polished, and a new Parallels Wizard feature (as well as the included tutorials) makes installation a snap—you can even purchase and download a copy of Windows 7 directly from within the setup program, which obviates the necessity of chasing down Windows installation disks. One noteworthy feature of Parallels Desktop 7 is that you can install the Windows 8 Developer Preview directly from within the application, a feature that VMware Fusion lacks. As Figure 1 shows, the Windows 8 Developer Preview option is in the lower right corner.

One of the most impressive new features is the integration of multi-touch gestures (introduced in OS X 10.7 Lion) into Windows 7. This feature works across other Windows applications as well. For example, it worked seamlessly with a trial edition of Microsoft Office 2010 that I installed. Other noteworthy features include the ability to use the Mac launch pad for Windows applications and share Mac OS X devices.

Parallels claims that it improved 3D performance in this latest release—a claim I was eager to test using the Windows version of the game *Quake 4*. Parallels Desktop 7 supports up to 1GB of video memory per virtual machine (VM) and enhanced audio support (up to 192kHz). It also supports the Windows 7 Aero interface. Overall, Parallels Desktop 7 has significantly improved in this area, and its performance approaches that of native Mac applications. However, office workers with fairly intense 3D hardware requirements (or Mac gamers looking to play Windows games on the side) will still be better off with a native PC with a fast discrete graphics card.

Besides testing 3D performance, I tested the Windows 8 Developer Preview using the built-in option. It installed and loaded without any problems. I have to admit it felt strange using multi-touch gestures to navigate through the Windows 8 Metro-style interface,

Figure 1: Parallels Desktop 7 VM creation screen

but the multi-touch gestures generally work, given the hardware limitation of my admittedly long-in-the-tooth test machine. Overall, VM performance was faster than I remember with previous versions, so Parallels has clearly done its homework here.

Both Parallels Desktop 7 and VMware Fusion 4.1 support USB devices, but only Parallels Desktop 7 offers an Enterprise Edition (for more than 100 annual licenses). This edition adds improved policy support for deployments and enhanced licensing options.

Parallels Desktop 7 for Mac

PROS: Fantastic 3D performance; improved stability over previous versions; speedy I/O and disk throughput; offers enterprise version with more IT-focused support features

CONS: Interface isn't quite as polished as VMware Fusion's interface

RATING: ◆◆◆◆◆

PRICE: $79.99

RECOMMENDATION: With superlative 3D performance, an available enterprise edition with enhanced functionality, and an integrated Windows 8 Developer Preview VM installation option, Parallels Desktop has emerged as the leading Mac virtualization product.

CONTACT: Parallels • 888-811-2489 or 425-282-6400 • www.parallels.com

VMware Fusion 4.1

I initially began my testing with VMware Fusion 4.0, but VMware Fusion 4.1 was released in the middle of my review process. Version 4.1 is a definite improvement over version 4.0, as the latter had some bugs and speed issues. Version 4.1 fixes those problems and brings other improvements, including changes to the native Lion full-screen mode.

Installing VMware Fusion 4.1 was quick and painless, and the video tutorials on the welcome screen make creating the first VMs straightforward. Both VMware Fusion 4.1 and Parallels Desktop 7 have improved their installation processes, but VMware's approach seems more streamlined and effective, especially with video training just a mouse-click away.

VMware Fusion 4.1 introduces a host of new features, including improved security options. For example, you can encrypt and password-protect VMs. Like Parallels Desktop 7, VMware Fusion 4.1 offers improved support for multi-touch gestures in OS X Lion. VMware Fusion 4.1 now utilizes the standard Lion full-screen button used in non-VM Windows, a change that makes switching to a full screen while running VMs much more intuitive. Based on my testing, both programs offer about the same level of multi-touch support, so neither program emerges as a winner in that department.

VMware Fusion 4.1 supports the Windows 7 Aero interface. VMware has revamped the way in which VMware Fusion 4.1 handles Windows applications, so managing program windows and VMs has a much more Mac-like feel. I prefer the way that VMware approaches handling programs and VM UI windows over the approach used by Parallels. This is largely a matter of personal preference, though.

VMware Fusion 4.1 boasts improved graphics performance, but Parallels Desktop 7 still has a slight edge over VMware Fusion 4.1, especially in the area of 3D graphics and games. VMware has made great strides in this area over the past few years—and the gap between the two competitors has narrowed significantly—but Parallels still wins the performance crown.

I ran Ubuntu Linux 11.10 on VMware Fusion 4.1 (see Figure 2) and Parallels Desktop 7. Both products ran Ubuntu without any problems. Performance was slow in spots, but I attribute that to aging test hardware rather than any inherent performance deficiency in either product.

Figure 2: VMware Fusion 4.1 running Ubuntu Linux 11.10

VMware Fusion 4.1

PROS: Polished full-screen interface options; easy integration with existing VMware virtualization products; vastly improved 3D performance over earlier version of the product

CONS: Still trails Parallels Desktop in overall speed and performance, especially in running 3D applications

RATING: ◆◆◆◆◇

PRICE: $49.99

RECOMMENDATION: VMware Fusion comes very close to matching the 3D performance of Parallels, and even exceeds it in some areas. IT shops with lots of VMware licenses might find it more convenient to stick with one vendor, and some people might prefer VMware's interface approach over the approach used by Parallels.

CONTACT: VMware • 877-486-9273 • www.vmware.com

Two Great Products

In my original comparison of these products a few years ago, I remarked how competition had improved both products considerably. It was true three years ago, and it's still true today. I picked Parallels Desktop as the winner in my last comparison, and my decision remains the same today. You can't go wrong with either product, but Parallels Desktop once again wins by a nose.

InstantDoc ID 142094

Jeff James (jjames@windowsitpro.com) is industry news analyst for *Windows IT Pro*. He was previously editor in chief of Microsoft *TechNet* magazine, was an editorial director at the LEGO Company, and has more than 15 years of experience as a technology writer and journalist.

AD Migration Tools

NetIQ Domain Migration Administrator vs. Quest Migration Manager for Active Directory

by Russell Smith

For anything but the smallest of networks, migrating to a new Active Directory (AD) domain can be a complex affair. You need to move users and network resources and modify desktop profiles to work with the new domain while simultaneously ensuring that users have seamless access to resources in both the old and new domains. Although it's possible to use Microsoft's free Active Directory Migration Tool (ADMT) to carry out complex migration projects, you'll find that for all but the simplest scenarios, it lacks some important features, such as the ability to migrate Security Descriptors (SDs) on organizational units (OUs), and has limited rollback capabilities. When undertaking an AD migration, it's all about planning and trying to minimize risk.

Once you get to the point where there are so many objects to migrate that it's not possible to move everything in one operation, having source and target domains coexist for a period of time allows for a phased migration. Migrating users based on how they work with one another and migrating resources based on how they're used often makes more sense than planning a migration around the physical location of objects. For these complex migration projects, you might consider using an AD migration tool, such as NetIQ Domain Migration Administrator or Quest Migration Manager for Active Directory. I recently evaluated these two products on the basis of their ease of installation and use, their features, and their documentation.

NetIQ Domain Migration Administrator

NetIQ Domain Migration Administrator is easy to install, although a SQL Server 2008 Enterprise, Standard, or Express database must be installed separately. You can install Domain Migration Administrator on any Windows server or client OS starting with Windows 2000 SP1. Agents can be deployed to any version of Windows starting with Win2K.

Figure 1 shows Domain Migration Administrator's GUI. Like ADMT, Domain Migration Administrator requires that you meet various prerequisites before an AD migration, such as creating secondary DNS zones so that source and target domains can be discovered, creating a trust between the two domains, and establishing the necessary cross-domain administrator permissions. Domain Migration Administrator doesn't walk you through these steps, but all the necessary information can be found in the documentation. Failure to meet the prerequisites results in basic operations failing, with cryptic, unhelpful error messages. Assuming the basic requirements have been met, Domain Migration Administrator offers to complete some other necessities on your behalf, such as creating AD$$$ groups and configuring auditing in each domain.

You can rename AD objects in the target domain if necessary, and you can specify how Domain Migration Administrator deals with naming conflicts. Objects in the source domain can also be set to auto-expire. After the user accounts are migrated, Domain Migration Administrator can create new passwords or copy users' existing passwords to a password server in the target domain.

Domain Migration Administrator includes database modeling, which lets you perform a trial migration to see what the potential results will be in the target domain. You'll be able to see what problems there might be and eliminate them from the actual migration. You can also use the database to clean up object information before importing it into the target domain, as Domain Migration Administrator pulls data from the source domain and uses the database as a temporary repository. Agents are dispatched to workstations to deal with migrating desktop profiles to work with the source domain.

NetIQ Domain Migration Administrator

PROS: Easy to set up; includes database modeling

CONS: Support for migrating application servers must be purchased separately; one-way directory synchronization

RATING: ◆◆◆◆◇

PRICE: $1,000 per 100-user license pack

RECOMMENDATION: A good choice for projects in which the requirements are clear and AD data needs to be cleaned up before migrating to a new domain.

CONTACT: NetIQ • 888-323-6768 or 713-548-1700 • www.netiq.com

Quest Migration Manager for Active Directory

Quest Migration Manager for Active Directory has a slightly different architecture from that of Domain Migration Administrator. Migration Manager uses Active Directory Application Mode (ADAM) to store migration information, which enables directory synchronization between the source and target domains. The Migration Manager installer package automatically installs ADAM if you choose the express install. The express install will also install SQL Server 2005 Express, which is needed if you intend to migrate Microsoft Exchange objects. However, there is one caveat: Even

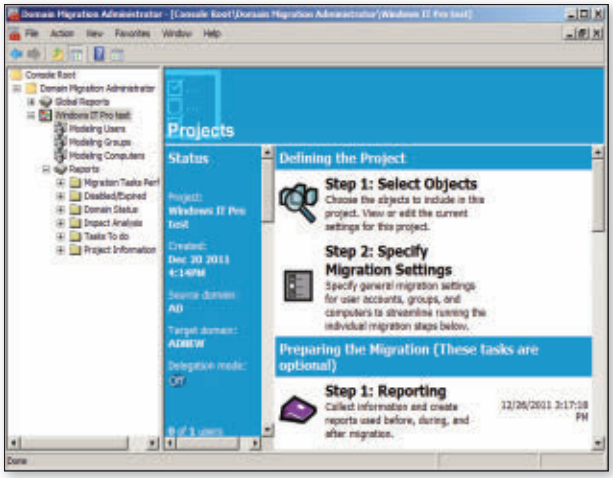


Figure 1: Domain Migration Administrator's GUI

Figure 2: Migration Manager's GUI

if you don't intend to migrate Microsoft Exchange Server objects, the installation will fail if the Messaging API (MAPI) client and Collaboration Data Objects (CDO) 1.2.1 aren't present. Migration Manager requires that source and target domains be Win2K SP2 or higher. Agents can be deployed to Windows Server or client OSs starting with Win2K.

I found Migration Manager's documentation to be comprehensive, although some topics weren't in a logical location. The Help files also include examples of commands that can be run to configure some of the prerequisites, such as disabling SID filtering and configuring the Windows Server firewall. Quest also includes a tips-and-tricks document, which is a vital read if you've never migrated AD to a new domain before. All the requirements are neatly listed, so it's clear exactly what's required before you start your migration project.

Migration Manager's GUI, which Figure 2 show, is more streamlined than that of Domain Migration Administrator. However, the Migration Manager GUI can be a little fussy in how it accepts certain information. For example, when trying to create a new domain migration pair, you have to enter the source domain information in a specific format before the wizard allows you to continue. The Browse buttons in the wizard don't work, forcing you to enter the information manually and in the correct format, which isn't very user friendly.

Although Migration Manager doesn't have a test database, there's a test mode in which no changes are made in the target domain. Instead, a report is generated to indicate whether the migration would be successful. While it's likely you'll need to set up only one migration project, multiple migration sessions can be configured to facilitate a phased migration. Migration sessions can't be copied in the GUI, but you can import or export objects for migration, which makes it much faster to create new migration sessions.

Migration Manager can migrate user passwords to the target domain. In addition, it can automatically synchronize AD objects, such as user accounts and groups. This greatly simplifies administration when source and target domains need to coexist for a period of time in order to migrate everything. Domain Migration Administrator also has sync capabilities, but they're one-way only.

Migration Manager has built-in support for migrating resources, including Microsoft System Center Configuration Manager (SCCM) and SQL Server. This functionality must be purchased separately with Domain Migration Administrator. Scheduled tasks can also be migrated, which isn't possible with Domain Migration Administrator.

Quest Migration Manager for Active Directory

PROS: Comprehensive resource support; feature rich

CONS: Not always user friendly

RATING: ◆◆◆◆◇

PRICE: $12 per migrated user (volume licensing available)

RECOMMENDATION: Quest has the edge over NetIQ, providing a more comprehensive feature set to cope with the most complex of scenarios.

CONTACT: Quest Software • 800-306-9329 or 949-754-8000 • www.quest.com

Editor's Choice

Both products take a project-based approach to AD migration and have comprehensive reporting. I preferred Migration Manager's simpler GUI and slightly easier setup. Plus, it has superior synchronization features that give more flexibility for larger migrations that require a long coexistence period.

Domain Migration Administrator has less support for migrating certain resources (e.g., SCCM), but it's a little more user friendly. For example, it has a friendly interface for tidying up objects and associated attribute information before being imported into the target domain. To achieve similar results in Migration Manager, you have to create text files with the necessary mapping information.

Although both products received the same rating, I've chosen Migration Manager as the Editor's Choice because its comprehensive feature set helps you manage a wider range of migration scenarios. Although it's slightly more expensive than Domain Migration Administrator, with the exception of Exchange, there's basic support for migrating some common network applications built in to the product.

InstantDoc ID 141928

Russell Smith
(rms@russell-smith.net) is an independent IT consultant specializing in systems management and security, and author of *Least Privilege Security for Windows 7, Vista and XP* (Packt).

Ultrabooks in the Enterprise

The market is about to experience a flood of thin, powerful, and highly portable computing devices

by Jeff James

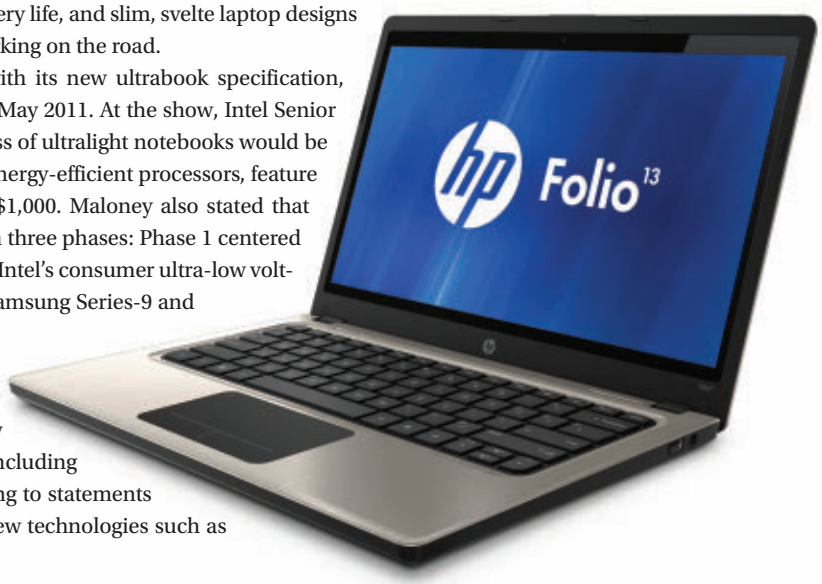
First released in early 2008, Apple's MacBook Air helped usher in a new era of ultralight portable computers. Other portable computers had been smaller and lighter, but few offered the winning combination of light weight, speedy boot time, thin form factor, and enough processing power to serve as a suitable replacement for a larger notebook that can accomplish most office tasks. Apple has refined and updated the MacBook Air several times over the past few years and continues to have sales success with the model. Digitimes Research pointed out that Apple was the only PC manufacturer to see its notebook sales increase in Q4 2012, selling 1.2 million units for the quarter.

But the MacBook Air isn't the only Apple product making waves in the PC industry. Thanks to the consumerization of IT, smartphones and tablets have been flooding into businesses at unprecedented rates, as employees begin to shift more of their workloads from traditional desktop and notebook PCs to tablets, smartphones, and ultralight notebooks. A recent survey of more than 2,500 *Windows IT Pro* readers revealed that close to 80 percent of respondents were allowing and/or supporting tablets in the office.

Enter the Ultrabook

Although the consumerization of IT can't be ignored—and some forward-thinking IT departments have found ways to support and encourage bring-your-own-device (BYOD) policies in the workplace—having employees use their own devices for work isn't an option for many companies and industries, including those that have to operate under stringent auditing and compliance regulations.

To add insult to injury, business laptops are often viewed as the boring, dependable, four-door rental sedans of the computing world, whereas laptops aimed at consumers could be categorized as the sporty red convertibles, boasting more attractive designs and leading-edge features such as SSD drives, backlit keyboards, and quicker boot-up times. It's not just a matter of simple aesthetics, as frequent travelers can attest: Lighter weight, longer battery life, and slim, svelte laptop designs translate to less fatigue and frustration when you're working on the road.



Intel hopes to help stack the deck in IT's favor with its new ultrabook specification, which was announced at the Computex trade show in May 2011. At the show, Intel Senior Vice President Sean Maloney claimed that this new class of ultralight notebooks would be powered by Intel's forthcoming "Ivy Bridge" family of energy-efficient processors, feature impressive thin-case designs, and retail for less than $1,000. Maloney also stated that Intel's ultrabook efforts would be rolled out primarily in three phases: Phase 1 centered on ultrabooks that launched in mid-2011 and that used Intel's consumer ultra-low voltage (CULV) second-generation core processors. (The Samsung Series-9 and Acer Aspire S3 ultrabooks fall into this category.)

Phase 2 ultrabooks are based on the Ivy Bridge processor family, which should be shipping in volume by April 2012. CES 2012 in January featured a raft of new ultrabook introductions that fall into this category, including the Acer Aspire S5, the HP Spectre, and more. According to statements by Maloney, phase 2 ultrabooks would also leverage new technologies such as USB 3.0 and Thunderbolt.

Finally, phase 3 ultrabooks would be based on Intel's upcoming "Haswell" chip architecture, which should ship sometime in 2013. Intel spokesperson Becky Emmett wrote in her Intel blog that Haswell would "... [reinvent] the capabilities of the laptop in ultra thin and light, responsive, and secure designs. With Haswell, Intel will transform the computing experience with more power-efficient processors that allow a more dynamic experience in insanely sleek systems."

Intel rival AMD is pushing a competing notebook design approach dubbed "ultrathin," which will be powered by AMD's new Trinity chipset (shipping in late Q2 or early Q3 2012). According to an article by Digitimes, Trinity-powered ultrathins could potentially arrive on the market with price tags "$100 to $200 lower than those of Intel's ultrabooks" (www.digitimes.com/news/a20120116PD219.html).

Ivy Bridge Ultrabooks

CES 2012 was a launch venue for many new ultrabooks that will be powered by the Ivy Bridge chipset. Here's a small sampling of some of the models (coming from a variety of manufacturers). These systems were announced at the show; they should all be shipping and available over the next few months.

Acer Aspire S5. Acer has already released the Acer Aspire S3 ultrabook, but the S5 promises an Ivy Bridge processor and even more capability.

Dell XPS 13. Dell has been a laggard in the ultrathin notebook category, with the overpriced (and tepidly received) Adamo series quietly being discontinued. The new Dell XPS 13 heralds Dell's more serious approach in the ultrabook space, with a more attractive design and an impressive feature set.

HP Spectre. Although aimed primarily at the consumer market—HP is pitching the more utilitarian Folio series to businesses—the Gorilla Glass–encased HP Spectre was one of the most attractive ultrabook designs to debut at CES.

Lenovo T430u. Lenovo has a long and storied history in the enterprise mobility market, thanks to the ubiquity of the stalwart Thinkpad series. The T430u aims to bring the Thinkpad brand into the ultrabook space.

Samsung Series 5. Samsung might not be a common PC brand in the enterprise, but the Series 5 could change that. Featuring a svelte case design and impressive specs, the Series 5 is feature-competitive with ultrabooks from Dell, HP, and Lenovo.

Ultrabooks for Businesses

Though most of the existing (and forthcoming) ultrabooks are aimed primarily at the consumer market, Intel hasn't forgotten about the business market, and it will begin shipping Ivy Bridge processors in mid-to-late 2012 that will support Intel vPro, which provides hardware-based management and security features aimed at IT professionals.

"We've been offering Intel vPro for the IT market for years, and upcoming Ivy Bridge processors will feature the sixth iteration of our vPro platform," Intel

Marketing Manager Roger Chang told me recently. "Intel vPro-based ultrabooks will help address the consumerization of IT and also give IT professionals the security and manageability they've been asking for."

One PC manufacturer that has taken an interest in providing ultrabooks tailored for the business market is HP, which released the Folio 13—a first-generation ultrabook—in December 2012.

"The Folio 13 might not be the thinnest or the lightest notebook, but we made design decisions to benefit business users," says Kyle Thornton, HP's category manager for ultralight business notebook PCs. "For example, we made the Folio 13 thick enough to offer a full RJ45 Ethernet jack, as many of our business customers hate using dongles and extra cables to provide that functionality when traveling. The Folio 13 weighs 3.3 pounds, but that extra weight goes to larger batteries that provide more than 9 hours of battery life."

Thornton added that HP made the decision to offer the Folio 13 in two variants, with one aimed at businesses and the other at consumers, with features appropriate for each market. For example, the Folio 13 business edition can be ordered with Windows 7 Professional and a trusted platform module (TPM) chip for enhanced security and manageability.

The Future of the Ultrabook

Intel plans to heavily promote the ultrabook concept with millions in marketing dollars throughout 2012. Intel has been the dominant player in the server, desktop, and traditional laptop markets, but all three of those areas are experiencing modest growth (or declines) as more consumers and businesses opt for smartphones, tablets, and ultralight notebooks. This trend is a troubling one for Intel because many Android smartphones and tablets are powered by processors developed by ARM, whereas most newer iPhones and all iPads rely on Apple's internally developed A4/A5 mobile processors.

So Intel is fighting back by working with OEM partners to develop more attractive ultrabook notebook designs, and by pushing more ultrabooks into the enterprise to help IT professionals stem the tide of consumer-focused devices flooding into offices. Intel clearly hopes the ultrabook initiative will help the company surf on top of the IT-consumerization tidal wave rather than be crushed by it. Regardless of whether Intel, AMD, or other players emerge as winners in the ultraportable notebook space in the months and years to come, it's clear that consumers and IT pros will soon have a flood of thin, powerful, and highly portable computing devices to choose from—a development that's good news for any consumer or corporation looking to purchase new portable PCs.

InstantDoc ID 141958

Jeff James
(jjames@windowsitpro.com) is industry news analyst for *Windows IT Pro*. He was previously editor in chief of Microsoft *TechNet* magazine, was an editorial director at the LEGO Company, and has more than 15 years of experience as a technology writer and journalist.

INSIGHTS FROM THE INDUSTRY

Information Security Issues

There are several information security problems that I think will take up a lot of IT administrators' time in the coming year. These emerging problems have affected the entire IT spectrum, not just information security. I see these problems as becoming drivers in our part of the industry, both from a customer demand and vendor offerings perspective. These information security problems include mobile, social, and cloud computing.

Mobile security has been a trending problem for a long time. It started back in 1983 with the first Compaq luggable. Since then, employees have been figuring out better ways to break out of the physical corporate walls to take their work data with them. And by better, I don't mean better for us in the information security field. The days of a secure physical network that exists only at work are long gone for most of us.

But laptops are the least of your worries when it comes to mobile computing these days. Small removable drives with a large capacity make the security risk presented by CD-ROMs and DVDs seem bite-sized in comparison. These devices are the new floppy disk, with people tracking in dirt from their home networks on USB drives.

And of course smartphones blur the line between what's deemed a computer and what's considered a personal device. iPhones, BlackBerries, and Android phones have most of the functionality of a desktop these days. Many companies are starting to let employees use their personal smartphones for work by letting them check email messages, log on to company intranets, and use VPNs. All of this presents particular challenges to the information security department, both now and going forward.

However, physical media and infrastructure is being eclipsed by the cloud. Companies are making use of these private or public clouds more than ever. Even big companies such as Zynga have begun using these services in lieu of deploying an in-house infrastructure, in order to cut costs and shorten deployment times. And although the cloud brings great conveniences to our infrastructure needs, the cloud also presents unique IT challenges.

When you're using cloud resources, you abdicate much of the information security function to a third party. You no longer have direct physical control over servers and OSs, so you have to trust your vendors to keep them updated and physically secure. And uptime for networks and servers is entirely dependent on the vendor.

Because of these challenges, service level agreements (SLAs) and due diligence become paramount when selecting a provider. But even selecting blue-chip vendors doesn't eliminate risk. The largest cloud provider, Amazon, has had several well-publicized outages—and credits to your bill only go so far. When using cloud services, always remember: Let the buyer beware.

When it comes to employees, most of their lives are stored online these days. This means that they can access their photo albums, songs, movies, and other media from a web browser inside your corporate network. What's your company's legal position if an employee is listening to pirated music that's streamed over the cloud on the company network? These are things that you'll have to deal with in the new age of cloud computing.

Social media has invaded our information security lives in all kinds of ways. First, the social apps are a technology that everybody loves but that drive security folks crazy. Facebook is the obvious one that comes to mind, but there's also Twitter, Foursquare, LinkedIn, and other programs that let users fritter away the work day checking up on their high school flames, networking for a new job, or playing inane games involving virtual gardens.

If social media were just productivity and bandwidth drains, that would be one thing—but they're also vectors for all kinds of attacks, such as fraud, security leaks, and regulatory problems. And just like the web, we can't always simply ignore or block these attacks.

Employees often need to use social applications for marketing and other legitimate purposes. Look for companies to produce specialized software and hardware to block, filter, and otherwise control these nuisances, while other companies offer products and services to increase companies' use of social apps for sales, marketing, and support. And the genre will continue to morph and become a bigger part of our personal and corporate e-lives no matter how you deal with it.

It's a brave new world out there in information security, and it's no longer just about keeping viruses and hackers out and corporate data in. More and more, it's about keeping data safe and finding ways to manage data in the cloud. The landscape is changing rapidly, and you'll have to be quick on your feet to stay ahead of these trending issues.

—Tony Howlett

InstantDoc ID 141753

Litigation Hold Updates in Exchange Server 2010 SP2

Reading the TechNet article "What's New in Exchange 2010 SP2" (http://tinyurl.com/7efk7d4), I was interested to note something that received zero attention (as far as I can tell) from customers during the Exchange Server 2010 SP2 development cycle. Buried at the end of the article is the following statement:

> In Exchange 2010 SP2, you can't disable or remove a mailbox that has been placed on litigation hold. To bypass this restriction, you must either remove litigation hold from the mailbox, or use the new IgnoreLegalHold switch parameter when removing or disabling the mailbox. The IgnoreLegalHold parameter has been added to the following cmdlets:
> - Disable-Mailbox
> - Remove-Mailbox
> - Disable-RemoteMailbox
> - Remove-RemoteMailbox
> - Disable-MailUser
> - Remove-MailUser

Litigation hold first appeared as a new feature in Exchange 2010 alongside Dumpster 2.0, a complete revamp of the way that the Exchange Information Store handles deleted user items. Because it's a reasonably new feature, you'd expect that Microsoft would have some tweaking to do based on customer feedback, and that's exactly what seems to have occurred here.

The whole point of a litigation hold is to preserve information in order to respond to legal discovery actions. Clearly this can't happen if an administrator accidentally deletes a mailbox that's on a litigation hold. Exchange 2010 SP2 stops this from happening by requiring an administrator to explicitly request to override the litigation hold on a mailbox or mail user when the administrator removes or disables the object. Of course, Exchange 2010 supports audit tracking for administrator actions so you can always find out exactly who deleted an object, provided that auditing is enabled and the person who deletes the object doesn't delete the audit item!

Interestingly, I don't see the Remove-StoreMailbox cmdlet listed in the set of updated cmdlets that support the Ignore LegalHold switch. Remove-StoreMailbox appeared in Exchange 2010 SP1 and is roughly equivalent to running Remove-Mailbox with the Permanent switch because it immediately and permanently removes a mailbox from its host database. By comparison, the normal use of Remove-Mailbox is to soft delete a mailbox so it can be recovered and reconnected to an Active Directory (AD) user object, providing that this operation occurs within the deleted mailbox retention period (usually anything from 14 to 30 days on production databases). Perhaps Microsoft decided that when an administrator runs Remove-StoreMailbox, he or she has already made the decision to blow away all traces of the mailbox and won't be concerned whether it's under litigation hold. Or maybe it's just an oversight.

—Tony Redmond

InstantDoc ID 141560

Windows Defender, Windows 8, and Trial Anti-Malware Applications

In his MSDN blog post "Protecting you from malware" (http://tinyurl.com/3gbxf3b), Steven Sinofsky says that Windows 8 will include an improved version of the Windows Defender anti-malware software. This means that all computers running Windows 8 will have up-to-date anti-malware protection. Microsoft has also indicated that if a third-party anti-malware application is installed on a computer running Windows 8, Windows Defender will essentially deprecate itself in favor of the alternative.

As you can probably guess, when Windows 8 releases, OEMs will continue to provide trial subscriptions from anti-malware vendors with the machines that they ship. This happens because anti-malware vendors provide OEMs with compensation for including trial versions of their software with new machines.

The study cited in Sinofsky's blog post found that 12 months after Windows 7 was released, 24 percent of Windows 7 computers didn't have up-to-date anti-malware software. This was down from almost 100 percent of computers having anti-malware software at release to manufacturing. The proposed hypothesis was that 25 percent of people had let their initial trial subscription expire. There's no real reason to believe that people running Windows 8 will be any more diligent about keeping their anti-malware subscriptions current compared to people running Windows 7. This suggests that 12 months after the release of Windows 8, approximately 25 percent of computers running Windows 8 won't have up-to-date anti-malware definitions.

Although Windows 8 will be able to detect when someone hasn't updated his or her definitions, I suspect it's unlikely that the OS will prompt the user with something along the lines of "You've let Virus Annihilator expire; do you want to renew your subscription, or do you want Windows Defender to take over from here?" It would be cool if it did, but I suspect that such a useful behavior would cause current anti-malware vendors to lose their biscuits.

Now that Windows 8 ships with an anti-malware solution, it's possible that by including trial software on computers running Windows 8 (and hence deprecating Windows Defender which, if left alone in the first place, would likely keep itself up-to-date), anti-malware vendors might be making some people's computers less secure in the long term.

—Orin Thomas

InstantDoc ID 141770

Microsoft Financing to Help Cash-Strapped IT Departments

With the global economy still in the doldrums, beleaguered IT professionals and IT managers are struggling to do more with less. Part of their strategy for staying afloat revolves around sticking with legacy software that's still getting the job done, such as the legion of IT departments that are opting to stay with Windows XP rather than upgrade to Windows 7. Computer hardware is also cheaper and more powerful than ever, a situation that leads many businesses to solider on with older equipment that's still getting the job done.

Yet not every IT department can afford to stay with legacy hardware and software systems, and sometimes—for the sake of ensuring critical business tasks or functions—new investments must be made in IT resources. Recognizing that businesses might need help in financing new software and hardware purchases, Microsoft has ramped up promotion of its Microsoft Financing arm that provides a number of financial services for Microsoft customers. To get the latest on what Microsoft Financing can offer customers, I recently spoke with Seth Eisner, general manager of Microsoft Financing.

Eisner mentioned that Microsoft Financing generally helps customers with three different financial scenarios. "We can help customers map their payments to deployments, or help them align financing around their budget cycles," Eisner said. "We also help customers with periodic payments that work [more effectively] with their cash flow situation . . . our financing options allow us to help customers buy more, buy better, buy bigger, and buy more often."

In a statement included in a news release as part of the renewed publicity push for Microsoft Financing, Microsoft partner Steria—a provider of IT business services in Europe—said that Microsoft Financing has helped the company streamline its IT operations. "We've known about financing but not for software," says Phillip Cournot, purchasing officer at Steria. "We've used other sources to procure our hardware, so when we learned about the Microsoft financing capabilities we were sold on the convenience. This is by far the best and most flexible financing solution we've used for purchasing our software and services."

According to Cournot, Microsoft Financing helped Steria update its enterprise licensing agreement to let flexible payments stretch over a three-year period, a change that more closely matches the actual deployment of the company's software. "My core IT challenge is to deploy Microsoft Office and Windows across our enterprise and reduce IT costs," says Christian Revelli, Group Chief Information Officer at Steria. "Microsoft Financing helped me in this task by splitting the cost of the rollout over three years."

—Jeff James

InstantDoc ID 141807

Lync Mobile Clients from Microsoft Debut

It took a year after the release of Microsoft Lync 2010, but Microsoft finally released mobile clients for its real-time communications server in December 2011. With these clients, users can access their corporate Lync server for IM, presence information, and related goodies, from their smartphones. Microsoft has released clients for Windows Phone and Android, with iPhone, iPad, and Symbian versions on the way.

Of course, these mobile client releases from Microsoft are no major surprise. "This was always part of the Microsoft roadmap that those clients were going to be later," said Scott Gode, vice president of product management and marketing for managed services provider, Azaleos. "Microsoft has been talking about them, so it's not a huge surprise that they're coming out when they are, but it's good to have them nonetheless."

Can you imagine Microsoft Exchange Server without a Microsoft client for email? It makes sense that Microsoft would provide its own Lync clients, as well; the Lync desktop version has been available since the server product launched—and it's a nice upgrade from the Office Communicator interface of Lync's predecessor, Office Communications Server (OCS). Users can join Lync conferences from the road on their smartphones as well—although it appears that will be audio only for the time being, no video.

Although it's good news to see that Microsoft's mobile Lync clients are available, other companies have been offering mobile clients, most notably Xync from Damaka, which is available for iOS, Android, and Symbian. "These third-party apps come out and plug right in and work right away after you buy them," said Tim Harrington, Lync architect for Azaleos. Which begs the question: Why would Microsoft delay releasing its own mobile clients? Is this delay a mistake, giving third parties the chance to stake their spots in the marketplace?

Something else to consider is that to use Microsoft's mobile Lync clients, you'll have to apply the latest updates available for Lync to your server environment. Cumulative Update 4 includes new mobility support, upon which Microsoft's clients rely—a requirement previous apps didn't have. Harrington also said, "Microsoft is going to require not only the CU4 update but also DNS and certificate changes as well for your Lync deployment. They haven't made it easy. Hopefully, they have a bigger picture in mind. So maybe some fancy whiz-bang functionality is going to come along that's going to require these changes."

Microsoft hasn't mentioned anything whiz-bang worthy that I've seen, which doesn't mean it's not under wraps somewhere. One thing's for certain: If you're running Lync 2010 and plan to support these clients, you might have a bit of work to do. And your smartphone-addicted end users might not be patient to get these apps running on their favorite devices.

—B. K. Winstead

InstantDoc ID 141642

AD INDEX

For detailed information about products in this issue of *Windows IT Pro*, visit the websites listed below.

VENDOR DIRECTORY

The following vendors or their products are mentioned in this issue of *Windows IT Pro* on the pages listed below.

DIRECTORY OF SERVICES | WINDOWS IT PRO NETWORK

Search our network of sites dedicated to hands-on technical information for IT professionals.
www.windowsitpro.com

Support

Join our discussion forums. Post your questions and get advice from authors, vendors, and other IT professionals.
www.windowsitpro.com/go/forums

News

Check out the current news and information about Microsoft Windows technologies.
www.windowsitpro.com/go/news

EMAIL NEWSLETTERS

Get free news, commentary, and tips delivered automatically to your desktop.

DevProConnections UPDATE
Exchange & Outlook UPDATE
Security UPDATE
SharePoint Pro UPDATE
SQL Server Pro UPDATE
Windows IT Pro UPDATE
WinInfo Daily UPDATE

www.windowsitpro.com/email

RELATED PRODUCTS

Custom Reprint Services

Order reprints of *Windows IT Pro* articles:
penton@wrightsmedia.com

Windows IT Pro VIP

Get exclusive access to over 40,000 articles and solutions on CD and via the web. Includes FREE access to eBooks and archived eLearning events, plus a subscription to either *Windows IT Pro* or *SQL Server Pro*.
www.windowsitpro.com/go/vipsub

SQL SERVER PRO

Explore the hottest new features of SQL Server, and discover practical tips and tools.
www.sqlmag.com

ASSOCIATED WEBSITES

DevProConnections

Discover up-to-the-minute expert insights, information on development for IT optimization, and solutions-focused articles at DevProConnections.com, where IT pros creatively and proactively drive business value through technology.
www.devproconnections.com

SharePoint Pro

Dive into Microsoft SharePoint content offered in specialized articles, member forums, expert tips, and web seminars mentored by a community of peers and professionals.
www.sharepointpromag.com

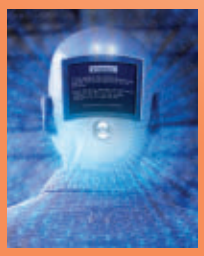
NEW WAYS TO REACH *WINDOWS IT PRO* EDITORS:

LinkedIn: To check out the *Windows IT Pro* group on LinkedIn, sign in on the LinkedIn homepage (www.linkedin.com), select the Search Groups option from the pull-down menu, and use "Windows IT Pro" as your search term.

Facebook: We've created a page on Facebook for *Windows IT Pro*, which you can access at: http://tinyurl.com/d5bquf. Visit our Facebook page to read the latest reader comments, see links to our latest web content, browse our classic cover gallery, and participate in our Facebook discussion board.

Twitter: Visit the *Windows IT Pro* Twitter page at www.twitter.com/windowsitpro.

Windows IT Pro



Ctrl+Alt+Del

by Jason Bovberg

"Send your funny screenshots, oddball product news, and hilarious end-user stories to rumors@windowsitpro.com. If we use your submission, you'll receive a *Windows IT Pro* Rubik's Cube."

No, I Will Not Fix Your Computer

PRODUCT OF THE MONTH

You've heard it a hundred times from your friends and family members—even from your end users about their home systems. Just because you're the computer whiz at work, you're automatically everyone's tech helper. Yes, your job description dictates that you have to fix other people's computers, but that doesn't mean you're on call 24 hours a day for everyone in your life! The good folks at ThinkGeek offer a tee-shirt that should help you with the problem. Learn more at www.thinkgeek.com/tshirts-apparel/unisex/itdepartment/388b.

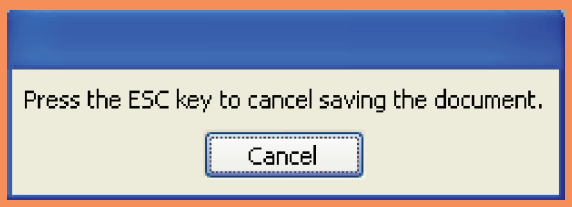


Figure 1: I'm confused

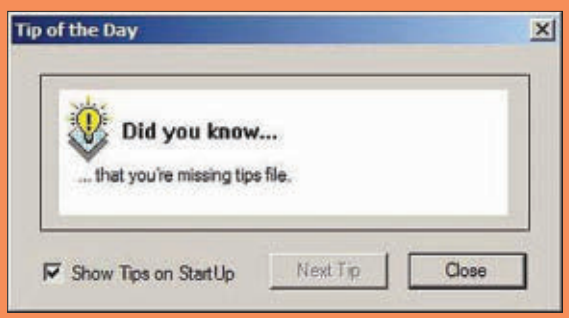


Figure 2: Do you have a tip for finding it?

USER MOMENT OF THE MONTH

In my previous job, I had a manager who forgot where he saved a file. He searched through his folders and couldn't find it. I suggested he check the Recycle Bin. I looked over to find him pulling the blue container from under his desk and rifling through the paper in it to find his missing spreadsheet. The most amazing part of this story? He was the IT manager for the company.

—Bob Robinson

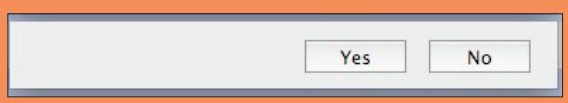


Figure 3: Well, of course, Yes!

March 2012 issue no. 211, *Windows IT Pro* (ISSN 1552-3136) is published monthly. *Windows IT Pro,* 748 Whalers Way, Fort Collins, CO 80525, (800) 793-5697 or (970) 663-4700. Sales and Marketing Offices: 748 Whalers Way, Fort Collins, CO 80525. Advertising rates furnished upon request. Periodicals Class postage paid at Fort Collins, Colorado, and additional mailing offices. **POSTMASTER: Send address changes to *Windows IT Pro,* 748 Whalers Way, Fort Collins, CO 80525.** SUBSCRIBERS: Send all inquiries, payments, and address changes to *Windows IT Pro,* Circulation Department, 748 Whalers Way, Fort Collins, CO 80525. Printed in the USA.

we're not just making servers. we're making server history.

While innovation comes rapidly in the IT industry, basic server architectures haven't changed for decades. That's why Cisco answered the need for innovation by introducing the Cisco Unified Computing System – which integrates compute, high-speed networking, storage access and virtualization in one system. Since its introduction, IT departments have dramatically reduced data center complexity while:

- Lowering operating costs by up to 30%
- Reducing Microsoft deployment times from weeks to minutes
- Harnessing the power of the UCS architecture for Microsoft Window Server and Exchange, SharePoint, and SQL Server deployments

The Cisco Unified Computing System, powered by intelligent Intel® Xeon® processors, signals the next evolution of the data center – where everything, and everyone, works together like never before.

Find out more at www.cisco.com/go/microsoft

together we are the human network. cisco.

Microsoft

Meetings from a laptop.
File sharing in the cloud.
Closing deals by videoconference.
It all works together.

Introducing Microsoft Office 365. Collaborate in the cloud with Office, Exchange, SharePoint, and Lync videoconferencing. **Starting as low as $10 per user per month. Begin your free trial now at Microsoft.com/office365**

Scan tag with a smartphone to learn about the Office 365 free trial.
Download the free scanner app at http://gettag.mobi

Microsoft® Office 365